Spring August 2014

GALOIS THEORY OF ITERATED MORPHISMS ON REDUCIBLE ELLIPTIC CURVES AND ABELIAN SURFACES WITH REAL MULTIPLICATION

Domenico Aiello

University of Massachusetts - Amherst

GALOIS THEORY OF ITERATED MORPHISMS ON REDUCIBLE ELLIPTIC CURVES AND ABELIAN SURFACES WITH REAL MULTIPLICATION

A Dissertation Presented

by

DOMENICO AIELLO

Submitted to the Graduate School of the
University of Massachusetts Amherst in partial fulfillment
of the requirements for the degree of

DOCTOR OF PHILOSOPHY

May 2014

Department of Mathematics and Statistics

GALOIS THEORY OF ITERATED MORPHISMS ON REDUCIBLE ELLIPTIC CURVES AND ABELIAN SURFACES WITH REAL MULTIPLICATION

A Dissertation Presented

by

DOMENICO AIELLO

Approved as to style and content by:

Siman Wong, Chair

Farshid Hajir, Member

Tom Weston, Member

David Mix Barrington
(Computer Science), Outside Member

Michael Lavine, Department Head
Mathematics and Statistics

Dedication

To my parents, for working so hard to provide me with limitless opportunity.

ACKNOWLEDGEMENTS

I would first like to thank my advisor, Siman Wong, for his mentorship these past few years. His guidance, humor, patience, honesty, and support have truly been appreciated. I would also like to thank my committee members, David Mix Barrington, Farshid Hajir, and Tom Weston, for the help and advice they have imparted. To every math teacher I have ever had - particularly, Eduardo Cattani, Susan Loepp, Steven J. Miller, Frank Morgan, and Jenia Tevelev - I offer my sincerest thanks for cultivating my love of math and inspiring my mathematical journey.

I am indebted to my friends - including the Fitz gang, the Route 9 Diner algebra crew, and the Google Hangout crowd - for the camaraderie, the food, and the ample math breaks we have shared over the years. I cannot imagine surviving grad school without you.

Lastly, my deepest gratitude belongs to my family for their continued love and support. Most importantly, I am eternally grateful to my parents, John and Rosemary Aiello, my sister, Amanda Aiello, and my twin brother, Enzo Aiello for always being there for me to provide comfort, distraction, and an undying source of encouragement. Though they may never read this thesis, it would never have been written without them.

ABSTRACT

GALOIS THEORY OF ITERATED MORPHISMS ON

REDUCIBLE ELLIPTIC CURVES AND

ABELIAN SURFACES WITH REAL MULTIPLICATION

MAY 2014

DOMENICO AIELLO, B.A., WILLIAMS COLLEGE

M.S., UNIVERSITY OF MASSACHUSETTS AMHERST

Ph.D., UNIVERSITY OF MASSACHUSETTS AMHERST

Directed by: Professor Siman Wong

Let F be a number field and let A be an abelian algebraic group defined over F. For a prime ℓ and a point $\alpha \in A(F)$, we obtain the tower of extensions $F([\ell^n]^{-1}(\alpha))$ by adjoining to F the coordinates of all the preimages of α under multiplication by $[\ell^n]$. This tower contains the coordinates of all of the ℓ-power torsion points of A along with a Kummer-type extension. The Galois groups of these extensions encode information about the density of primes $\mathcal{P}$ in the ring of integers of F for which the order of α (mod $\mathcal{P}$) is not divisible by ℓ. In this thesis, we determine these Galois groups and explicitly compute the associated density for the cases where A is (1) a reducible elliptic curve; (2) a product of elliptic curves with complex multiplication; (3) an abelian surface with real multiplication.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF NOTATION

F	base field
A (or E)	abelian variety (or elliptic curve) defined over F
ℓ	fixed prime
α	specified point in $A(F)$
U_n	$[\ell^n]^{-1}(\alpha)$, the preimages of α under multiplication by ℓ^n
β_n	distinguished point in U_n satisfying $[\ell^n]\beta_n = \alpha$ and $[\ell]\beta_n = \beta_{n-1}$
T_n	$F(A[\ell^n])$, the ℓ^nth torsion field
K_n	$F([\ell^n]^{-1}(\alpha)) = T_n(\beta_n)$, the ℓ^nth Kummer field
T_∞	$\cup_{n=1}^{\infty} T_n$
K_∞	$\cup_{n=1}^{\infty} K_n$
$G_{T_n/F}$	$\mathrm{Gal}(T_n/F)$, the torsion part
G_{K_n/T_n}	$\mathrm{Gal}(K_n/T_n)$, the Kummer part
$G_n = G_{K_n/F}$	$\mathrm{Gal}(K_n/F)$
$N^{(n)}$	$\mathrm{Gal}(T_\infty/T_n)$
ρ	$G_{T_\infty/F} \longrightarrow \mathrm{Aut}(T_\ell(A))$, the ℓ-adic torsion representation
ρ_{ℓ^n}	$G_{T_n/F} \longrightarrow \mathrm{Aut}(A[\ell^n])$, the (mod ℓ^n) torsion representation
κ	$G_{K_\infty/T_\infty} \longrightarrow T_\ell(A)$, the Kummer map
κ_n	$G_{K_n/T_n} \longrightarrow A[\ell^n]$, the (mod ℓ^n) Kummer map
ω	$G_{K_\infty/F} \longrightarrow T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$, the arboreal representation
ω_n	$G_{K_n/F} \longrightarrow A[\ell^n] \rtimes \mathrm{Aut}(A[\ell^n])$, the (mod ℓ^n) arboreal representation
$\mathcal{F}(G)$	density of primes $\mathcal{P}$ such that the order of α (mod $\mathcal{P}$) is not divisible by ℓ

CHAPTER 1

INTRODUCTION

Let F be a number field and let A be an abelian algebraic group defined over F. For a prime ℓ and a point $\alpha \in A(F)$, the tower of extensions $F([\ell^n]^{-1}(\alpha))$ contains the coordinates of all of the ℓ-power torsion points of A along with a Kummer-type extension. The action of the absolute Galois group $G_{\bar{\mathbb{Q}}/F}$ on this tower encodes density information about the order of $\alpha \pmod{\mathcal{P}}$ for $\mathcal{P}$ a prime ideal in the ring of integers of F.

In this thesis, our first goal is to compute this density for each of the following cases of A:

(1) an elliptic curve for which $A[\ell]$ has a $G_{\bar{\mathbb{Q}}/F}$-invariant subgroup,

(2) a product of elliptic curves with complex multiplication,

(3) an abelian surface with real multiplication.

In pursuit of this goal, let T_∞ be the union of all the ℓ-power torsion fields $F(A[\ell^n])$ of A and K_∞ be the union of the extensions $F([\ell^n]^{-1}(\alpha))$. Note that $G_{K_\infty/F}$ has as a quotient the Galois group $G_{T_\infty/F}$, which is given by its action on the Tate module $T_\ell(A)$ of A. This is the well studied ℓ-adic torsion representation $\rho : G_{T_n/F} \to \mathrm{Aut}(T_\ell(A))$. The kernel of this quotient map is isomorphic to a subgroup of $T_\ell(A)$. We therefore obtain a map $\omega : G_{K_\infty/F} \to T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$, called the arboreal representation. The second goal of this thesis is to determine the possible images of the arboreal representation.

1.1 History of the Problem

In his *Disquisitiones Arithmeticae*, Gauss observed that the decimal expansion of $1/7 = 0.142857\ 142857\ 142857\ldots$ has a "large" period length of six, whereas $1/11 = 0.09\ 09\ 09\ldots$

has a period length of only two. He determined that for any prime $p \neq 2, 5$, the period length of the decimal expansion of $1/p$ is the smallest nonnegative integer k satisfying $10^k \equiv 1 \pmod{p}$, called the *order* $\pmod{p}$. Since Fermat's Little Theorem says that $10^{p-1} \equiv 1 \pmod{p}$, the largest period of $1/p$ occurs when $k = p - 1$. In this case, he called 10 a *primitive root* $\pmod{p}$ and inquired how often 10 is a primitive root $\pmod{p}$ as p varies over all of the primes [15].

More generally, for any prime p and any positive integer a not divisible by p, one can examine the period length of the base a expansion of $1/p$. Analogous to above, $1/p$ will have the largest possible period length of $p - 1$ when a is a primitive root $\pmod{p}$; that is, when the smallest nonnegative integer k satisfying $a^k \equiv 1 \pmod{p}$ is $p - 1$. It can then be asked how often a is a primitive root $\pmod{p}$ as p varies over all of the primes. In a conversation with Hasse in 1927 [1], Artin conjectured that for any a that is neither -1 nor a perfect square, there exist infinitely many p for which a is a primitive root $\pmod{p}$. He further hypothesized that the number of such primes up to x is asymptotic to $C_a \frac{x}{\log x}$, where C_a is a constant depending on a. Still largely unsolved, Artin's Conjecture has applications to many areas of mathematics, including group theory, algebraic and analytic number theory, and algebraic geometry [15]. While it is known there exists an a for which Artin's Conjecture holds, no single such a has been specifically determined [4], [7].

For a fixed prime ℓ and an element α in an abelian group A defined over $\mathbb{Q}$, one can investigate the density of primes p for which the order of $\alpha \pmod{p}$ is not divisible by ℓ. Such a question is of great interest in arithmetic dynamics, as it determines the density of primes p for which α is a periodic point $\pmod{p}$ under multiplication by ℓ (for the additive case) or raising to the ℓth power (for the multiplicative case). The multiplicative case $A = \mathbb{Q}^\times$ gives an analogue of Artin's Conjecture $\pmod{\ell}$, which was originally examined by Hasse in [5], [6] as well as by Moree in [13] and others. In the case where A is an abelian variety, the geometry of A engages with this problem and greatly influences the density. Significant progress has been achieved by Jones and Rouse in [10] for A an elliptic curve. Under natural constraints, they compute the density as a rational function of ℓ for a large class of elliptic curves defined over any global field F. Asymptotically, the density is $1 - O(\frac{1}{\ell})$.

In this thesis, we generalize the results of Jones and Rouse in several directions. First, we consider classes of elliptic curves not covered by the work of [10], called reducible elliptic curves. Second, we extend their results to the product of non-isogenous elliptic curves with complex mul-

tiplication. Lastly, we examine higher dimensional analogues of this (mod ℓ) Artin's Conjecture by studying abelian surfaces with real multiplication. In each case, we investigate how the geometry and field theory affect this problem and compute the desired density as a rational function of ℓ.

1.2 Background

Let F be a number field with ring of integers $\mathcal{O}_F$. Let A/F be an abelian variety of dimension d and choose a non-torsion point α on A defined over F. For a fixed prime ℓ, we are interested in $\mathcal{F}(G)$, the density of primes $\mathcal{P}$ in $\mathcal{O}_F$ for which the order of α (mod $\mathcal{P}$) is not divisible by ℓ. This density is encoded by the Galois theory associated to the abelian variety. We therefore translate our problem into the language of field theory.

For each positive integer n, let $U_n = [\ell^n]^{-1}(\alpha) = \{\beta \in A(\bar{\mathbb{Q}}) : [\ell^n]\beta = \alpha\}$ be the set of all preimages of α under multiplication by ℓ^n. It is well known that $U_n \cong (\mathbb{Z}/\ell^n)^{2d}$ [14, p. 39]. Let K_n be the field obtained by adjoining to F the coordinates of each element of U_n. Since any two members of U_n differ by an ℓ^n-torsion point, each K_n contains the ℓ^n-torsion field, $T_n = F(A[\ell^n])$. Indeed, if for each n we distinguish $\beta_n \in U_n$ such that $[\ell]\beta_{n+1} = \beta_n$, then $K_n = T_n(\beta_n)$.

For a given prime $\mathcal{P}$ in $\mathcal{O}_F$ not ramifying in K_n, let $k_\mathcal{P} = \mathcal{O}_F/\mathcal{P}$ and $\bar{\alpha} \in A(k_\mathcal{P})$ be the reduction of α (mod $\mathcal{P}$). The order of $\bar{\alpha}$ is not divisible by ℓ — that is, $[\ell^m]\bar{\alpha} = \bar{\alpha}$ for some m — if and only if for each n there exists $\gamma \in A(k_\mathcal{P})$ such that $[\ell^n]\gamma = \bar{\alpha}$. This latter statement occurs if and only if the action of $\mathrm{Frob}_\mathcal{P}$ on U_n has a fixed point for all n. Letting $G_{K_n/F} = \mathrm{Gal}(K_n/F)$, by the Chebotarev Density Theorem, the density of such primes $\mathcal{P}$ is

$$\mathcal{F}(G) = \lim_{n\to\infty} \frac{\#\{\sigma \in G_{K_n/F} : \sigma \text{ fixes at least one } \beta \in U_n\}}{\#G_{K_n/F}}.$$

In this light, computing the density $\mathcal{F}(G)$ hinges on determining the possible Galois groups $G_{K_n/F}$. Since each $\sigma \in G_{K_n/F}$ restricts to an automorphism of $A[\ell^n]$ and defines an ℓ^n torsion point given by $\sigma(\beta_n) - \beta_n$, we obtain an injective homomorphism

$$\omega_n : G_{K_n/F} \to A[\ell^n] \rtimes \mathrm{Aut}(A[\ell^n]) \cong (\mathbb{Z}/\ell^n)^{2d} \rtimes \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n)$$

defined by $\omega_n(\sigma) = (\sigma(\beta_n) - \beta_n, \sigma\big|_{A[\ell^n]})$. Passing to the inverse limit gives what is called the *arboreal representation.*

To examine the possible images of the arboreal representation, we decompose it into two parts, the ℓ-adic torsion representation and the Kummer map. The *Kummer map* κ is the inverse limit of the maps $\kappa_n : G_{K_n/T_n} \to A[\ell^n]$ defined by $\kappa_n(\sigma) = \sigma(\beta_n) - \beta_n$. The torsion representation ρ has been significantly more studied and is the inverse limit of the maps $\rho_{\ell^n} : \mathrm{Gal}(T_n/F) \to \mathrm{Aut}(A[\ell^n]) \cong \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n)$ given by the action of $G_{T_n/F}$ on $A[\ell^n] \cong (\mathbb{Z}/\ell)^{2d}$. A fundamental result in the field is Serre's open image theorem [20], which says for A an elliptic curve without complex multiplication, the torsion representation is surjective for almost all ℓ. For more details regarding the torsion representation, the Kummer map, and the arboreal representation, see Chapter 2.

For A an elliptic curve defined over a global field F with surjective ℓ-adic torsion representation, Jones and Rouse in [10] provide necessary and sufficient conditions for when the arboreal representation will be surjective and in this case compute $\mathcal{F}(G)$. We summarize their results for the non-complex multiplication case below.

Proposition 1.1 ([10, Proposition 5.1],[20, IV, 3.4, Lemma 3])**.** *Let ℓ be a prime. The ℓ-adic representation $\rho : Gal(T_\infty/F) \to GL_2(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

(i) the base field F is linearly disjoint from $\mathbb{Q}(\zeta_{\ell^n})$ for all n;

(ii) $G_{T_1/F} \cong GL_2(\mathbb{Z}/\ell\mathbb{Z})$.

(iii) If $\ell = 2$ and D is the discriminant of the 2-division polynomial, then $-D$, $2D$, and $-2D$ are not squares in F, and the 4-torsion polynomial is irreducible and its Galois group has order 48 over F;

(iv) if $\ell = 3$, then the 9-division polynomial is irreducible over $F(\zeta_9)$.

Proposition 1.2 ([10, Theorem 5.2])**.** *Assume the ℓ-adic representation is surjective. Then the arboreal representation is surjective if and only if the following conditions hold:*

(i) the point $\alpha \notin \ell A(F)$;

(ii) if $\ell = 2$, then $F(\beta_1) \not\subseteq F(A[4])$.

In the case of surjective arboreal representation, computing the density $\mathcal{F}(G)$ hinges on the following.

Proposition 1.3 ([10, Theorem 3.8])**.** *Suppose that κ is surjective. Then we have*

$$\mathcal{F}(G) = \int_{im\rho} \ell^{-ord_\ell(det(M-I))} d\mu.$$

Here, $d\mu$ denotes the Haar measure on $im\rho$, normalized such that $\mu(im\rho) = 1$, and we take $ord_\ell(0) = \infty$.

Using the results above, the density $\mathcal{F}(G)$ is then computed.

Theorem 1.4 ([10, Theorem 5.5])**.** *Suppose the arboreal representation is surjective. Then*

$$\mathcal{F}(G) = \frac{\ell^5 - \ell^4 - \ell^3 + \ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}$$

Though the formalism of Jones and Rouse works for other elliptic curves and abelian varieties of higher dimension, it is too difficult to employ in general. For example, for an abelian variety of dimension $d > 1$, properties of the Weil pairing dictate that the image of ρ can be as large as $\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$. Even in the abelian surface case (so $d = 2$), the image of ρ as a subgroup of $\mathrm{GSp}_4(\mathbb{Z}_\ell)$ is much too large to utilize the methods in [10] to compute $\mathcal{F}(G)$. However, Jones and Rouse are able to determine necessary and sufficient conditions for when the image of the torsion representation is all of $\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$. In this case with $d = 2$, they compute bounds for $\mathcal{F}(G)$. Specifically, they show

$$\frac{\ell^7 - 2\ell^6 - \ell^5 + 4\ell^4 - 2\ell^3 + 2\ell^2 - 5}{(\ell^4 - 1)(\ell^2 - 1)(\ell - 1)} \leq \mathcal{F}(G) \leq \frac{\ell^7 - \ell^6 - \ell^5 + 3\ell^4 - 2\ell^3 + \ell^2 - 4}{\ell^7 - \ell^5 - \ell^3 + \ell}.$$

In this thesis, we investigate elliptic curves not explored by Jones and Rouse as well as higher dimensional abelian varieties in which the endomorphism ring reduces the size of the image of ρ. In each case, we compute the density $\mathcal{F}(G)$.

1.3 Outline of the Thesis

In Chapter 2 we provide more details regarding the maps mentioned in the previous section. In addition, we give a complete description of the subgroups of a semidirect product and give some background on abelian surfaces with real multiplication.

In Chapter 3 we explore reducible elliptic curves. Specifically, we consider two important subcases: one in which the elliptic curve A has an ℓ torsion point defined over F and another in which there is no ℓ torsion point over F, but still a $G_{T_\infty/F}$-invariant subgroup of $A[\ell]$ of order ℓ. We will assume in both cases that $G_{T_\infty/F}$ is as large as possible given these conditions; that is, using the isomophism $T_\ell(A) \cong \mathbb{Z}_\ell \times \mathbb{Z}_\ell$ and $\mathrm{Aut}(T_\ell(A)) \cong \mathrm{GL}_2(\mathbb{Z}_\ell)$, we will assume that either

$$\text{I. } \mathrm{im}\rho \cong \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}$$

or

$$\text{II. } \operatorname{im}\rho \cong \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}.$$

Let ω_n be the (mod ℓ^n) arboreal representation. For a 2 x 2 matrix $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell^n)$, define $a(M)$ to be a and $a_i(M)$ to be the coefficient of ℓ^i in the ℓ-adic expansion of a. Define $b(M)$, $b_i(M)$, $c(M)$, $c_i(M)$, $d(M)$, and $d_i(M)$ analogously. For reducible elliptic curves of Type I above, we have the following result toward our second goal:

Theorem 1.5. *Let $\ell > 3$ be a fixed prime. Let E/F be a reducible elliptic curve of Type I. Suppose $G_{T_n/F} \cong \{M \in GL_2(\mathbb{Z}/\ell^n) : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \ (mod\ \ell)\}$ and $\alpha \notin E(F) \cap \ell E(T_n)$. Then $im\omega_n$ is one of the following.*

(i) $E[\ell^n] \rtimes G_{T_n/F}$

(ii) $\left\{(v, M) \in E[\ell^n] \rtimes G_{T_n/F} : v \equiv \left(\begin{smallmatrix} 0 \\ \gamma_1 c_1(M) + \gamma_2(d_0(M)-1) \end{smallmatrix}\right) \ (mod\ \ell)\right\}$ *for some fixed $\gamma_1, \gamma_2 \in \mathbb{Z}/\ell$.*

We will then compute the density in each of these two cases. In particular, we prove the following:

Theorem 1.6. *If we are in case (i) in Theorem 1.5, then $\mathcal{F}(G) = \frac{\ell^3-\ell-1}{\ell^4+\ell^3-\ell-1}$. If we are in case (ii) and $\gamma_1 \equiv 0 \ (mod\ \ell)$, then $\mathcal{F}(G) = \frac{2\ell^3-\ell^2-2}{\ell^4+\ell^3-\ell-1}$. If we are in case (ii) and $\gamma_1 \not\equiv 0 \ (mod\ \ell)$, then $\mathcal{F}(G) = \frac{\ell^3-\ell^2-1}{\ell^4+\ell^3-\ell-1}$.*

We have similar results for Type II reducible elliptic curves:

Theorem 1.7. *Let $\ell > 3$ be a fixed prime. Let E/F be a reducible elliptic curve of Type II. Suppose $G_{T_n/F} \cong \{M \in GL_2(\mathbb{Z}/\ell^n) : M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \ (mod\ \ell)\}$ and $\alpha \notin E(F) \cap \ell E(T_n)$. Then $im\omega_n$ is one of the following.*

1. $E[\ell^n] \rtimes G_{T_n/F}$
2. $\left\{(v, M) \in E[\ell^n] \rtimes G_{T_n/F} : v \equiv \left(\begin{smallmatrix} * \\ (d_0(M)-1)\gamma \end{smallmatrix}\right) \ (mod\ \ell)\right\}$ *for a fixed $\gamma \in \mathbb{Z}/\ell$.*

Theorem 1.8. *If the conditions of Theorem 1.7. Then $\mathcal{F}(G) = \frac{\ell^5-2\ell^4+2\ell+1}{\ell^5-\ell^3-\ell^2+1}$ if we are in case (i) and $\mathcal{F}(G) = \frac{\ell^5-\ell^4-\ell^3-\ell^2+2\ell+2}{\ell^5-\ell^3-\ell^2+1}$ if we are in case (ii).*

In Chapter 4 we consider the case of products of elliptic curves with complex multiplication. We investigate the torsion representation and in the case of surjective Kummer map, compute the associated density.

In Chapter 5 we let A be an abelian surface with real multiplication. After determining necessary and sufficient conditions for when the arboreal representation surjects onto a particular set, we compute $\mathcal{F}(G)$. In particular, we prove the following:

Theorem 1.9. *Let A be an Abelian surface defined over $\mathbb{Q}$ and let F be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}$. Let ℓ be an inert prime and define $R_n = \mathcal{O}_\ell/(\ell^n)$. Let $R = \varprojlim R_n$. Fix $\alpha \in A(F)$. Assume the Kummer map κ is surjective and the torsion part satisfies $im\rho \cong \{M \in GL_2(R) : det(M) \in \mathbb{Z}_\ell^\times\}$. Then*

$$\mathcal{F}(G) = \frac{\ell^{15} - \ell^{13} - \ell^{11} + \ell^{10} + \ell^9 + \ell^3 + \ell^2 + 1}{\ell^{15} - \ell^{11} - \ell^4 + 1}.$$

We also provide explicit examples of abelian surfaces with real multiplication that satisfy the conditions of the above theorem.

Theorem 1.10. *Let $A = J_0(23)$. Then for all $\ell > 5$ inert in $\mathbb{Q}(\sqrt{5})$ there exists a quadratic twist A_d of A and $\alpha \in A_d$ satisfying the conditions of Theorem 1.9. Thus, the density of primes p for which the order of α $(mod\ p)$ is not divisible by ℓ is $\frac{\ell^{15}-\ell^{13}-\ell^{11}+\ell^{10}+\ell^9+\ell^3+\ell^2+1}{\ell^{15}-\ell^{11}-\ell^4+1}$.*

In the final chapter, we discuss several open questions and possible directions for future work.

CHAPTER 2

PRELIMINARIES

In this chapter we give some background material on the arboreal representation, which can be decomposed into the torsion representation and the Kummer map. We also provide a complete characterization of the subgroups of a semidirect product as well as a brief description of abelian surfaces with real multiplication. For a summary of the notation introduced here, see the List of Notation provided toward the end of this thesis.

2.1 The ℓ-adic Representation

We begin with a discussion of the ℓ-adic torsion representation associated to an abelian varietiy A of dimension $d \geq 1$ defined over a global field F. For a fixed prime ℓ we define $A[\ell^n]$ to be the kernel of the multiplication by ℓ^n map, denoted $[\ell^n]$. Note that $\mathrm{Gal}(F^{\mathrm{sep}}/F)$ acts on $A[\ell^n]$, so that for each n we obtain a representation

$$\rho_{\ell^n} : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}(A[\ell^n]).$$

Using the well known isomorphism $A[\ell^n] \cong (\mathbb{Z}/\ell^n)^{2d}$ [14, p. 39], we have $\mathrm{Aut}(A[\ell^n]) \cong \mathrm{GL}_{2d}(\mathbb{Z}/\ell^n)$. Passing to the inverse limit, we obtain the *ℓ-adic torsion representation*

$$\rho : \mathrm{Gal}(F^{\mathrm{sep}}/F) \to \mathrm{Aut}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$$

where $T_\ell(A) = \lim_{n \leftarrow \infty} A[\ell^n] \cong (\mathbb{Z}_\ell)^{2d}$ is the ℓ-adic Tate module.

The torsion representation has been studied extensively. In the case of $A = E$ an elliptic curve without complex multiplication, a well known theorem of Serre [20] says the torsion representation is surjective for almost all ℓ.

Theorem 2.1 ([20, Proposition, p. IV-19]). *Let $\rho : Gal(\bar{K}/K) \to \prod_\ell Aut(T_\ell)$, where the product is taken over the set of all prime numbers. Let $G = im\rho \subseteq \prod_\ell Aut(T_\ell)$ and $G_\ell = im(\rho_\ell) \subseteq Aut(T_\ell)$, so that G_ℓ is the image of G under the ℓth projection map. Let $\tilde{G}_\ell$ be the image of G_ℓ in $Aut(E_\ell) := Aut(T_\ell/\ell T\ell) \cong GL(2, \mathbb{F}_\ell)$. The following properties are equivalent:*

(i) G is open in $\prod_\ell Aut(T_\ell)$.

(ii) $G_\ell = Aut(T_\ell)$ for almost all ℓ.

(iii) $\tilde{G}_\ell = Aut(E_\ell)$ for almost all ℓ.

(iv) $\tilde{G}_\ell$ contains $SL(E_\ell)$ for almost all ℓ.

Theorem 2.2 ([20, Theorem, p. IV-20]). *Assume that the modular invariant j of E is not an integer of K. Then E enjoys the equivalent properties (i), (ii), (iii), (iv) of 2.1.*

For more information regarding the torsion representation for higher dimensional abelian varieties, see [19, Resume des cours de 1984-1985].

In [24], Swinnerton-Dyer determines an explicit list of *exceptional* primes for which ρ is not surjective and gives the possible images of ρ in each case. For example, he shows that there are three types of exceptional images of ρ, denoted by G [Corollary 1 to Lemma 2, Theorem 4]:

(i) G is contained in a Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; or

(ii) G is contained in the normalizer of a Cartan subgroup, but not in the Cartan subgroup itself; or

(iii) The projective image of G is isomorphic to S_4.

The exceptional primes of types (i) and (ii) can be explicitly determined; and there is an explicitly determinable finite set which contains the exceptional primes of type (iii).

2.2 The Kummer Map

Fix $\alpha \in A(F)$ and for each n choose $\beta_n \in [\ell^n]^{-1}(\alpha)$ such that $[\ell]\beta_{n+1} = \beta_n$. It is easy to see that $K_n := F([\ell^n]^{-1}(\alpha))$ is $T_n(\beta_n)$. We define the nth Kummer map, κ_n to be

$$\kappa_n : G_{K_n/T_n} \to A[\ell^n]$$

defined by $\kappa_n(\sigma) = \sigma(\beta_n) - \beta_n$.

Proposition 2.3. *The nth Kummer map is an injective homomorphism for all n.*

Proof. We first show κ_n is a homomorphism. Let $\sigma, \tau \in G_{K_n/T_n}$. Then

$$\begin{aligned}\kappa_n(\sigma\tau) &= \sigma\tau(\beta_n) - \beta_n \\ &= \sigma\tau(\beta_n) - \sigma(\beta_n) + \sigma(\beta_n) - \beta_n \\ &= \sigma(\tau(\beta_n) - \beta_n) + \sigma(\beta_n) - \beta_n \\ &= (\tau(\beta_n) - \beta_n) + (\sigma(\beta_n) - \beta_n)\end{aligned}$$

since $\tau(\beta_n) - \beta_n \in E[\ell^n]$ is in $E(T_n)$, which is fixed by σ. To see injectivity, note that if $\kappa_n(\sigma) = 0$, then σ fixes both T_n and β_n, so that σ fixes K_n and is thus trivial. □

Taking the inverse limit gives the *ℓ-adic Kummer map*

$$\kappa : G_{K_\infty/T_\infty} \to T_\ell(A)$$

where $K_\infty = \cup K_n$, $T_\infty = \cup T_n$, and $T_\ell(A) = \lim_{n \leftarrow \infty} A[\ell^n]$ is the ℓ-adic Tate module.

We now reinterpret the Kummer map in terms of group cohomology (see, for example, Section VIII in [23]). Consider the short exact sequence of $G_{\bar{\mathbb{Q}}/T_n}$-modules

$$0 \to A[\ell^n] \to A(\bar{\mathbb{Q}}) \xrightarrow{\ell^n} A(\bar{\mathbb{Q}}) \to 0.$$

This gives a long exact sequence that begins

$$0 \to A[\ell^n] \to A(T_n) \xrightarrow{\ell^n} A(T_n) \xrightarrow{\delta_n} H^1(G_{\bar{\mathbb{Q}}/T_n}, A[\ell^n]) \to H^1(G_{\bar{\mathbb{Q}}/T_n}, A(\bar{\mathbb{Q}})) \xrightarrow{\ell^n} H^1(G_{\bar{\mathbb{Q}}/T_n}, A(\bar{\mathbb{Q}})).$$

From the middle of this exact sequence, we obtain the *Kummer sequence*

$$0 \to \frac{A(T_n)}{\ell^n A(T_n)} \xrightarrow{\delta_n} H^1(G_{\bar{\mathbb{Q}}/T_n}, A[\ell^n]) \to H^1(G_{\bar{\mathbb{Q}}/T_n}, A(\bar{\mathbb{Q}}))[\ell^n] \to 0.$$

Note that the connecting homomorphism δ is defined to be $\delta_n(\alpha)(\sigma) = \sigma(\beta_n) - \beta_n$. This is known as the Kummer pairing and for fixed α is exactly the nth Kummer map defined above. Further, since $A[\ell^n]$ is contained in $A(T_n)$, we have

$$H^1(G_{\bar{\mathbb{Q}}/T_n}, A[\ell^n]) = \mathrm{Hom}(G_{\bar{\mathbb{Q}}/T_n}, A[\ell^n]),$$

so we obtain an injective homomorphism

$$A(T_n)/\ell^n A(T_n) \hookrightarrow \mathrm{Hom}(G_{\bar{\mathbb{Q}}/T_n}, A[\ell^n])$$

defined by $\alpha \mapsto \kappa_n(\cdot)$.

Though the Kummer map is a familiar object, the Galois theory of the corresponding tower of fields has been significantly less studied than the torsion representation. As a result, less is known about the possible images of κ. In the special case where A is an elliptic curve and the Kummer map is surjective, Jones and Rouse in [10] are able to compute the density $\mathcal{F}(G)$ by computing a particular integral (see Section 2.3). One of the goals of this thesis is to determine possible images of the Kummer map in the case where the torsion representation is not surjective.

2.3 The Arboreal Representation and the Density $\mathcal{F}(G)$

The β_n as defined in the previous section define a rooted tree with root α when we assign edges according to the action of $[\ell]$; that is, β is adjacent to β' if and only if $[\ell]\beta' = \beta$. Recall that we obtain the field K_n by adjoining the coordinates of the nth level of this rooted tree: $K_n = F([\ell^n]^{-1}(\alpha))$ and $K_\infty = \cup K_n$. Let $G_n = G_{K_n/F}$ and $G = G_{K_\infty/F}$. Note that G acts on our rooted tree and G_n is the quotient of G obtained by restricting the action of G to the first n levels of the tree. Since G is profinite, it has a natural Haar measure μ, which we normalize to have total mass 1. We can now ask what density of $\sigma \in G$ fix an entire branch of our rooted tree, which we denote $\mathcal{F}(G)$. That is,

$$\begin{aligned}\mathcal{F}(G) &= \mu\{\sigma \in G : \sigma \text{ fixes a branch of tree } \} \\ &= \lim_{n\to\infty} \frac{\#\{\sigma \in G_n : \sigma(\beta) = \beta \text{ for some } \beta \in [\ell^n]^{-1}(\alpha)\}}{\#G_n}\end{aligned}$$

This limit exists since the above sequence is bounded and monotonically decreasing.

To compute this density, we study the Galois theory of the extension K_∞/F. To that end, for each $n \geq 1$ we combine the torsion representation and the Kummer map to obtain a homomorphism

$$\omega_n : \mathrm{Gal}(K_n/F) \to A[\ell^n] \rtimes \mathrm{Aut}(A[\ell^n])$$

defined by $\omega_n(\sigma) = (\sigma(\beta_n) - \beta_n, \sigma\big|_{A[\ell^n]})$. Passing to the inverse limit gives the *arboreal representation*

$$\omega : \mathrm{Gal}(K_\infty/F) \to T_\ell(A) \rtimes \mathrm{Aut}(T_\ell(A))$$

where $T_\ell(A) = \lim_{n\leftarrow\infty} A[\ell^n]$ is the Tate module of A.

We now translate the definition of the density $\mathcal{F}(G)$ into the language of the arboreal representation. To give a better understanding of the density $\mathcal{F}(G)$ and how it is computed, we include the following, the statement and argument of which appear in the proof of Theorem 3.8 in [10].

Proposition 2.4. $\mathcal{F}(G) = \lim_{n\to\infty} \dfrac{\#\{(v,M) \in im(\omega_n) : v \in im(M-I)\}}{\#im\omega_n}$.

Proof. We frequently use the fact that if $X \in M_d(\mathbb{Z}_\ell)$ acts on $V = \mathbb{Z}_\ell^d$ with $\det(X) \neq 0$, then the image of $X : V \to V$ has index $\ell^{\mathrm{ord}_\ell(\det(X))}$. Note that if $\det(M-I) = 0$, then by the convention $\mathrm{ord}_\ell(0) = \infty$, we have $\ell^{-\mathrm{ord}_\ell(\det(M-I))} = 0$.

Suppose that $\sigma \in G_{K_n/F}$ and $\omega_n(\sigma) = (v, M) \in (\mathbb{Z}/\ell^n\mathbb{Z})^d \rtimes \mathrm{GL}_d(\mathbb{Z}/\ell^n\mathbb{Z})$. If $\beta \in U_n$, then σ fixes β if and only if $\sigma(\beta) - \beta_n = \beta - \beta_n$. Write $\beta = \beta_n + \gamma$, where $\gamma \in A[\ell^n]$. Then $\sigma(\beta) = \sigma(\beta_n) + \sigma(\gamma)$, so

$$\sigma(\beta) - \beta_n = \sigma(\beta_n) - \beta_n + \sigma(\gamma).$$

The right-hand side equals $\beta - \beta_n$ if and only if $\sigma(\beta_n) - \beta_n + \sigma(\gamma) = \gamma$. If $\omega_n(\sigma) = (v, M)$, then this means that $v + M(\sigma) = \sigma$, whence $(M-I)(-\sigma) = v$. This occurs if and only if v is in the image of $M - I$.

If $M \in G_{T_n/F}$ with $\det(M-I) \not\equiv 0 \pmod{\ell^n}$ and $\tilde{M}$ is any lift of M to $G_{T_\infty/F}$, then $\mathrm{ord}_\ell(\det(\tilde{M}-I)) = \mathrm{ord}_\ell(\det(M-I))$. Therefore, the index of the image of $M-I$ (acting on $(\mathbb{Z}/\ell^n\mathbb{Z})^d$) and the index of the image of $\tilde{M}-I$ (acting on $\mathbb{Z}_\ell^d$) are the same. It follows that the index of the image of $\det(M-I)$ is $\ell^{\mathrm{ord}_\ell(\det(M-I))}$. Hence, the number of elements of $G_{K_n/F}$ fixing some point of U_n divided by the size of $G_{K_n/F}$ is given by

$$\frac{\#\{(v,M) \in \mathrm{im}(\omega_n) : v \in \mathrm{im}(M-I)\}}{\#\mathrm{im}\omega_n}.$$

Our result now follows. □

Computing the density $\mathcal{F}(G)$ therefore relies on determining the possible images of the arboreal representation. To do so, we refer to several results from [10], which we reproduce below.

Proposition 2.5 ([10, Theorem 3.4])**.** *Let $G_{T_n/F} = Gal(T_n/F)$. Suppose that, for some $m \geq 1$, the following hold:*

(i) $A[\ell^m]/A[\ell^{m-1}]$ is irreducible as a $G_{T_m/F}$-module;

(ii) $\alpha \notin A(F) \cap \ell A(T_n)$ for all $n \geq m$.

Then $im\omega_n \cong A[\ell^n] \rtimes G_{T_n/F}$ for all $n \geq m$.

Proposition 2.6 ([10, Lemma 3.6]). *Let $N^{(n)} = Gal(T_\infty/T_n)$, so $N^{(n)}/N^{(n+1)} \cong Gal(T_{n+1}/T_n)$. If $n \geq 1$ and $Hom_{G_{T_1/F}}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0$, then $A(F) \cap \ell A(T_n) = A(\mathbb{Q}) \cap \ell A(T_{n+1})$.*

Proposition 2.7 ([10, Lemma 3.7]). *Suppose that there is a normal subgroup H of $G_{T_1/F}$ with order coprime to ℓ and $A[\ell]^H = 0$. Then $A(F) \cap \ell A(T_1) = \ell A(F)$.*

Proposition 2.8 ([10, Theorem 3.8]). *Suppose that κ is surjective. Then we have*

$$\mathcal{F}(G) = \int_{im\rho} \ell^{-ord_\ell(det(M-I))} d\mu.$$

Here, $d\mu$ denotes the Haar measure on $im\rho$, normalized such that $\mu(im\rho) = 1$, and we take $ord_\ell(0) = \infty$.

2.4 Subgroups of Semidirect Products

To determine the possible images of the arboreal representation, we will first need to describe all subgroups of a semidirect product, $G = U \rtimes_\varphi H$ for groups U and H and homomorphism $\varphi : H \to \mathrm{Aut}U$.

Definition 2.9. *We say that subgroups L of U and R of H form an internal φ_U^H-pair (or an I-pair for short) in the group $G = U \rtimes_\varphi H$ if there exists a map $\theta : R \to U$ such that*

(i) for all $g, h \in H$ there exists $u \in L$ for which $\theta(gh) = u \cdot \theta(g) \cdot \varphi(g)(\theta(h))$

(ii) for all $u \in L$ and $h \in R$, we have $\theta(h) \cdot \varphi(h)(u) \cdot \theta(h)^{-1} \in L$.

For each I-pair (L, R, θ) we define the set $L \rtimes_{\varphi,\theta} R = \{(u \cdot \theta(h), h) : u \in L, h \in R\}$, called the fiber-crossed product of this pair.

We now summarize the results from [25], which says that I-pairs fully describe the subgroups of $G = U \rtimes_\varphi H$. Our proof is modified slightly in structure and notation from the original.

Theorem 2.10 ([25, Theorem, p. 984]). *The subgroups of G are exactly the fiber-crossed products of all its I-pairs.*

Proof. Let (L, R) be an I-pair for G. We show that $L \rtimes_{\varphi,\theta} R$ is a subgroup of G. Indeed,

$$\begin{aligned}(u_1 \cdot \theta(h_1), h_1)(u_2 \cdot \theta(h_2), h_2) &= (u_1 \cdot \theta(h_1) \cdot \varphi(h_1)(u_2 \cdot \theta(h_2)), h_1 h_2) \\ &= (u_1 \cdot \theta(h_1) \cdot \varphi(h_1)(u_2) \cdot \theta(h_1)^{-1} \cdot \theta(h_1) \cdot \varphi(h_1)(\theta(h_2)), h_1 h_2) \\ &= (u_1' \cdot \theta(h_1) \cdot \varphi(h_1)(\theta(h_2)), h_1 h_2),\ u_1' \in L \qquad \text{(condition (ii))} \\ &= (u_1'' \cdot \theta(h_1 h_2), h_1 h_2),\ u_1'' \in L. \qquad \text{(condition (i))}\end{aligned}$$

Now let Γ be a subgroup of G. Let $L = \Gamma \cap U$ and $R = \{h \in H : \text{ there exists } u \in U \text{ such that } (u, h) \in \Gamma\}$. We show (L, R) forms an I-pair for G by explicitly constructing θ.

For each coset xL in Γ/L, select an element $\bar{x}$ as representative. Letting p_1 be projection from Γ onto the first factor, we define $\theta(h) = p_1(\bar{x})$, where $x = (u, h) \in \Gamma$. Certainly, this is a well-defined map $\theta : R \to U$. Furthermore, note that $(u, h) = (u \cdot \theta(h)^{-1} \cdot \theta(h), h)$, where $u \cdot \theta(h)^{-1} \in L$.

All that is left to show is that θ satisfies conditions (i) and (ii) in Definition 2.9. Let $u \in L$ and $h_1, h_2 \in H$. To see condition (i), note that

$$(\theta(h_1) \cdot \varphi(\theta(h_2)) \cdot \theta(h_1 h_2)^{-1}, 1) = (\theta(h_1), h_1)(\theta(h_2), h_2)(\theta(h_1 h_2), h_1 h_2)^{-1}$$

is in Γ, so that $\theta(h_1) \cdot \varphi(\theta(h_2)) \cdot \theta(h_1 h_2)^{-1}$ is in L as desired. Similarly, for condition (ii), we note that

$$(\theta(h_1) \cdot \varphi(h_1)(u) \cdot \theta(h_1)^{-1}, 1) = (\theta(h_1), h_1)(u, 1)(\theta(h_1), h_1)^{-1}$$

is in Γ, so that $\theta(h_1) \cdot \varphi(h_1)(u) \cdot \theta(h_1)^{-1}$ is in L. □

2.5 Abelian Surfaces

An abelian variety A is a (connected) projective abelian algebraic group. Let d be its dimension. For $d > 1$, the arboreal representation $\omega : G_{\bar{\mathbb{Q}}/\mathbb{Q}} \to \mathbb{Z}_\ell^{2d} \rtimes \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$ will never be surjective. This is because the ℓ-adic representation ρ will not be surjective. Indeed, the Galois invariance and non-degeneracy of the Weil pairing implies that $G_{T_n/F} \subseteq \mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n\mathbb{Z})$, the group of symplectic similitudes. For more information about abelian varieties, see [8, Section A.7].

Jones and Rouse [10] determine the following criteria for when ρ surjects onto $\mathrm{GSp}_{2d}(\mathbb{Z}_\ell)$. Here, $\Phi : A \to \hat{A}$ is a polarization defined over F.

Proposition 2.11 ([10, Proposition 6.1]). *Let $d \geq 2$ and let ℓ be a prime such that $gcd(\ell, \#ker(\Phi))$ is 1. Then, the ℓ-adic torsion representation $\rho : G_{T_\infty/F} \to GSp_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

(i) F is linearly disjoint from $Q(\zeta_{\ell^n})$ for all n;

(ii) $G_{T_1/F} \cong GSp_{2d}(\mathbb{Z}/\ell\mathbb{Z})$;

(iii) if $\ell = d = 2$, then T_1 is linearly disjoint from $\mathbb{Q}(\sqrt{2}, i)$.

Jones and Rouse also give criteria for when the map to the Kummer part is surjective:

Proposition 2.12 ([10, Theorem 6.2]). *Let $d \geq 2$ and let ℓ be a prime such that $gcd(\ell, \#ker(\Phi)) = 1$. Suppose the ℓ-adic representation $\rho : G_{T_\infty/F} \to GSp_{2d}(\mathbb{Z}_\ell)$ is surjective. Then the ℓ-adic Kummer map $\kappa : G_{K_\infty/T_\infty} \to \mathbb{Z}_\ell^{2d}$ is surjective if and only if the following conditions hold:*

(i) $\alpha \notin \ell A(F)$;

(ii) if $\ell = 2$, then $\beta_1 \notin A(T_1)$.

Putting the above two results together, we obtain the following:

Corollary 2.13 ([10, Corollary 6.3]). *The arboreal representation*

$$\omega : G_{K_\infty/F} \longrightarrow (\mathbb{Z}_\ell)^{2d} \rtimes GSp_{2d}(\mathbb{Z}_\ell)$$

is surjective if and only if the conditions of Propositions 2.11 and 2.12 are satisfied.

If $d = 2$, A is called an abelian surface. Even in this simplest case, working with the image of ρ inside $\mathrm{GL}_4(\mathbb{Z}_\ell)$ is too difficult to employ the results of [10]. Jones and Rouse are, however, able to obtain the following bounds in the case of $G_{K_\infty/F} \cong \mathbb{Z}_\ell^4 \rtimes \mathrm{GSp}_4(\mathbb{Z}_\ell)$:

$$\frac{\ell^7 - 2\ell^6 - \ell^5 + 4\ell^4 - 2\ell^3 + 2\ell^2 - 5}{(\ell^4 - 1)(\ell^2 - 1)(\ell - 1)} \leq \mathcal{F}(G) \leq \frac{\ell^7 - \ell^6 - \ell^5 + 3\ell^4 - 2\ell^3 + \ell^2 - 4}{\ell^7 - \ell^5 - \ell^3 + \ell}.$$

Unfortunately, Jones and Rouse are not able to compute the exact density in any case. A theorem of Ribet [17], however, can be applied for abelian surfaces with real multiplication; that is, abelian surfaces for which $\mathrm{End}(A) \otimes \mathbb{Q}_\ell$ is a real extension of $\mathbb{Q}_\ell$ (it is known that this extension will be quadratic). We now restate Ribet's theorem in the special case of A an abelian surface with real multiplication.

Theorem 2.14 ([17, Theorem 3.1]). *Let G be the image of ρ inside $GL_4(\mathbb{Z}_\ell)$ and let $R_\ell = End(A) \otimes_{\mathbb{Z}} \mathbb{Z}_\ell$. Then G is isomorphic to a subgroup of $H = \{x \in GL_2(R_\ell) : det(x) \in \mathbb{Z}_\ell^\times\}$. Furthermore, $G \cong H$ for almost all ℓ.*

Though the coefficient ring R_ℓ is bigger than $\mathbb{Z}_\ell$, working with two-by-two matrices will allow us to use modified versions of the results from [10] to explicitly compute $\mathcal{F}(G)$.

To give a concrete example of an abelian surface A and a prime ℓ for which Ribet's theorem holds, we will need to determine the possible images of the torsion representation. We do so by finding the possible determinant one subgroups of the image of the torsion representation. We will need the following, which lists the maximal subgroups of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$.

Let $V \cong \mathbb{F}_\ell^2$ be a two-dimensional vector space over $\mathbb{F}_\ell$. Then we have the following possible maximal subgroups G of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ [3].

I. **Parabolic (Borel) subgroups.** G is any subgroup conjugate to the group of non-singular upper triangular matrices. Thus, $G \cong \mathbb{F}_{\ell^2} \rtimes \mathbb{F}_{\ell^2}^\times$.

II. **Stabilizers of subspace decompositions.** Write $V = V_1 \oplus V_2$, where V_1 and V_2 are linear subspaces of V. Then G is a stabilizer of these decompositions. In particular, G is of the form

$$(\mathrm{GL}_1(\mathbb{F}_{\ell^2}) \times \mathrm{GL}_1(\mathbb{F}_{\ell^2})) \rtimes S_2 \cong \mathrm{GL}_1(\mathbb{F}_{\ell^2}) \wr S_2$$

intersected with $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$. In this case, G is isomorphic to the dihedral group D_{ℓ^2-1} of order $2(\ell^2-1)$. (G is not maximal when $\ell = 3$.)

III. **Field extension subgroups.** $\mathbb{F}_{\ell^4}$ is naturally a vector space over $\mathbb{F}_{\ell^2}$, therefore $\mathrm{Aut}(\mathbb{F}_{\ell^4}) \hookrightarrow \mathrm{GL}_2(\mathbb{F}_{\ell^2})$. Since $\mathrm{Aut}(\mathbb{F}_{\ell^4}) \cong \mathbb{F}_{\ell^4}^\times$ is cyclic, we will get a cyclic group of order dividing $\ell^4 - 1$. It turns out that $\mathrm{Aut}(\mathbb{F}_{\ell^4}) \cap \mathrm{SL}_2(\mathbb{F}_{\ell^2}) \cong \mathbb{Z}/(\ell^2+1)$ is cyclic of order ℓ^2+1. The Galois group $G_{\mathbb{F}_{\ell^4}/\mathbb{F}_{\ell^2}}$ acts on these points as outer automorphisms and this action is defined over $\mathbb{F}_{\ell^2}$. This gives $G \cong D_{\ell^2+1}$. (G is not maximal when $\ell = 3$.)

IV. **Subfield subgroups.** Note $\mathrm{SL}_2(\mathbb{F}_\ell) \hookrightarrow \mathrm{SL}_2(\mathbb{F}_{\ell^2})$. We obtain $G \cong \mathrm{SL}_2(\mathbb{F}_\ell).2$; that is, G is a group with a normal subgroup isomorphic to $\mathrm{SL}_2(\mathbb{F}_\ell)$ of index two. There are two conjugates of this maximal subgroup inside $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$. ($G$ is not maximal when $\ell = 2$.)

V. **Exceptional subgroups** The projective image of G is isomorphic to either A_4, S_4, or A_5.

CHAPTER 3

REDUCIBLE ELLIPTIC CURVES

3.1 Preliminaries

Let F be a number field and let A be an abelian algebraic group of dimension d defined over F. For a prime ℓ and a point $\alpha \in A(F)$, the tower of extensions $F([\ell^n]^{-1}(\alpha))$ contains all of the coordinates of the ℓ-power torsion points of A along wtih a Kummer-type extension. The action of the absolute Galois group, $G_{\bar{\mathbb{Q}}/F}$ on this tower encodes density information about the order of $\alpha \pmod{\mathcal{P}}$ for $\mathcal{P}$ a prime ideal in the ring of integers of F. When A is an elliptic curve, Jones and Rouse [10] determine necessary and sufficient conditions for the Galois action on the tower $F([\ell^n]^{-1}(\alpha))$ to be as large as possible and under these conditions compute the associated density.

The Galois group $G := G_{K_\infty/F}$ encodes information regarding the density of primes $\mathcal{P}$ in the ring of integers of F such that the order of $\alpha \bmod \mathcal{P}$ is coprime to ℓ. Letting $G_n = G_{K_n/F}$, we define this density to be

$$\mathcal{F}(G) = \lim_{n\to\infty} \frac{\#\{\sigma \in G_n : \sigma \text{ fixes at least one } \beta \in [\ell^n]^{-1}(\alpha)\}}{\#G_n}.$$

Computing $\mathcal{F}(G)$ therefore depends on determining the possible images of the arboreal representation. To do so, we decompose the arboreal representation into two parts, the torsion representation and the Kummer map. The torsion representation $\rho : G_{T_\infty/F} \to \mathrm{Aut}(T_\ell(A)) \cong \mathrm{GL}_{2d}(\mathbb{Z}_\ell)$ has been studied extensively. In the case of A an elliptic curve without complex multiplication, the torsion representation is known to be surjective for almost all ℓ [20]. Though the Kummer map $\kappa : G_{K_\infty/T_\infty} \to A[\ell^n]$ is a familiar object — as mentioned in Chapter 2, it is the connecting homomorphism in the Kummer sequence — the Galois theory of the corresponding tower of fields is not well understood, and we do not know much about the possible images of κ. In the special case where the Kummer map is surjective, Jones and Rouse [10] were able to compute the density $\mathcal{F}(G)$ by using Proposition 2.8.

In this chapter, we examine elliptic curves E for which the action of the absolute Galois group on the tower of extensions $F([\ell^n]^{-1}(\alpha))$ is not as large as possible. One way to obtain this is to consider elliptic curves for which the torsion representation ρ is not surjective. In particular, we study elliptic curves with an ℓ-torsion point defined over F as well as elliptic curves for which an ℓ-order subgroup of $E[\ell]$ is invariant under the action by $G_{\bar{F}/F}$. Specifically, we consider elliptic curves for which either

$$\text{I. } \mathrm{im}\rho = \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}$$

or

$$\text{II. } \mathrm{im}\rho = \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}.$$

The main difficulty is determining the possible images of the ℓ-adic Kummer map. Doing so allows us to determine the possible images of the arboreal representation so that we may use Proposition 2.8 to compute the associated density.

Remark 3.1. We note here that there is a concrete way we can generate examples of reducible elliptic curves E/F of Type I or II. By Serre's Open Image Theorem [20], a given elliptic curve E/L without complex multiplication will have surjective ℓ-adic torsion representation for almost all ℓ. Fix an ℓ such that E/L has surjective ρ. Let $F \subseteq L(E[\ell])$ be the degree $\ell^2 - 1$ (resp. $\ell + 1$) extension of L such that E contains an ℓ-torsion point over F (resp. $E[\ell]$ contains a $G_{\bar{Q}/F}$-invariant subgroup of order ℓ). Then E/F is a reducible elliptic curve of Type I (resp. Type II).

We will need the following results to determine the possible images L of the Kummer map for both Type I and Type II reducible elliptic curves, so we prove them here.

Proposition 3.2. *Let L be a $G_{T_n/F}$-invariant submodule of $E[\ell^n] \cong \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^n$. Then one of the following holds.*

(1) $L = E[\ell^n]$

(2) $L = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$

(3) $L \subseteq E[\ell^{n-1}] = \left\langle \left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle.$

Proof. We prove by induction. First let $n = 1$. Our $G_{T_1/F}$-invariant subspace of $E[\ell]$ can be of dimension 0, 1, or 2. If it is of dimension 0, then $L = 0$ and we are in case (3). If it is

of dimension 2, then $L = E[\ell]$ and we are in case (1). We therefore only have to consider $G_{T_1/F}$-invariant subspaces of dimension 1, which is equivalent to finding all non-zero common eigenvectors of the matrices $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. It is clear that all such vectors are in $\left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \right\rangle$, so we are indeed in case (2).

Let $n > 1$ and suppose now that the above holds for all $n > m \geq 1$. We show it for $n = m$. Let L be a $G_{T_n/F}$-invariant submodule of $E[\ell^n]$. Then ℓL is a T_{n-1}-invariant submodule of $E[\ell^{n-1}]$. Using $\ell L \subseteq L$ and our inductive hypothesis, as a subset of $E[\ell^n] = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right) \right\rangle$, we have $\ell L = E[\ell^{n-1}] = \left\langle \left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$, $\ell L = \left\langle \left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell^2 \end{smallmatrix}\right) \right\rangle$, or $\ell L \subseteq E[\ell^{n-2}] = \left\langle \left(\begin{smallmatrix} \ell^2 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell^2 \end{smallmatrix}\right) \right\rangle$. In the first case, L contains the vectors $\left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right)$ as well as a preimage of each of the form $\left(\begin{smallmatrix} 1+x_1\ell^{n-1} \\ y_1\ell^{n-1} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x_2\ell^{n-1} \\ 1+y_2\ell^{n-1} \end{smallmatrix}\right)$, respectively. It is clear then that L contains both $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$, so $L = E[\ell^n]$.

In the second case, we have L contains the vectors $\left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ \ell^2 \end{smallmatrix}\right)$ as well as a preimage of each of the form $\left(\begin{smallmatrix} 1+x_1\ell^{n-1} \\ y_1\ell^{n-1} \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} x_2\ell^{n-1} \\ \ell+y_2\ell^{n-1} \end{smallmatrix}\right)$, respectively. For $n > 2$, this implies L contains both $\left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right)$. Since ℓL does not contain $\left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right)$ we conclude L does not contain $\left(\begin{smallmatrix} 0 \\ 1 \end{smallmatrix}\right)$ so that $L = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$. If $n = 2$, the above implies that $\left\langle \left(\begin{smallmatrix} \ell \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 1 \\ t\ell \end{smallmatrix}\right) \right\rangle \subseteq L \subseteq \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$ for some $t \in (\mathbb{Z}/\ell)^\times$. A quick check by hand shows that indeed $L = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$.

Finally, if $\ell L \subseteq E[\ell^{n-2}]$, then certainly $L \subseteq E[\ell^{n-1}]$. □

We use the proof of Theorem 3.4 in [10] to eliminate case (3) in Proposition 3.2 by adding an extra assumption on α. We will show in the following section that the possible subgroups L above are precisely the possible images of the nth Kummer map. Thus if $L \subseteq E[\ell^{n-1}]$, then we have $\mathrm{im}\kappa_n \subseteq E[\ell^{n-1}]$.

Proposition 3.3. *Suppose $\alpha \notin E(F) \cap \ell E(T_n)$. Then $\mathrm{im}\kappa_n$ cannot be contained in $E[\ell^{n-1}]$.*

Proof. We have the following commutative diagram with exact rows [23]:

$$\begin{array}{ccccc} 0 & \longrightarrow & E(T_n)/\ell^n E(T_n) & \xrightarrow{\delta_n} & H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell^n]) \\ & & \downarrow & & \downarrow{\scriptstyle \ell^{n-1}} \\ 0 & \longrightarrow & E(T_n)/\ell E(T_n) & \xrightarrow{\delta_1} & H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell]). \end{array}$$

Here $\delta_n(\alpha)$ is the element of $H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell^n])$ represented by the 1-cocycle $\sigma \mapsto \sigma(\beta_n) - \beta_n$. If $\mathrm{im}\kappa_n \subseteq E[\ell^{n-1}]$, then $\delta_n(\alpha)$ lies in the kernel of $[\ell^{n-1}] : H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell^n]) \to H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell])$. This implies that $\delta_1(\alpha) = 0$, which means $\alpha \in E(F) \cap \ell E(T_n)$, contradicting our assumption.

□

3.2 Images of the Arboreal Representation for Type I Reducible Elliptic Curves

In this section, we determine the possible images of the arboreal representation for an elliptic curve E/F with an ℓ torsion point defined over F. In particular, we aim to prove the following.

Theorem 3.4. *Let $\ell > 3$ be a fixed prime. Let E/F be a reducible elliptic curve of Type I. Suppose $G_{T_n/F} = \{M \in GL_2(\mathbb{Z}/\ell^n) : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}$ and $\alpha \notin E(F) \cap \ell E(T_n)$. Then $\mathrm{im}\omega_n$ is one of the following.*

(i) $E[\ell^n] \rtimes G_{T_n/F}$

(ii) $\left\{(v, M) \in E[\ell^n] \rtimes G_{T_n/F} : v \equiv \left(\begin{smallmatrix} * \\ \gamma_1 c_1(M) + \gamma_2 (d_0(M) - 1) \end{smallmatrix}\right) \pmod{\ell}\right\}$ *for some fixed* $\gamma_1, \gamma_2 \in \mathbb{Z}/\ell$.

Applying the results of Section 2.4 to our situation, we see that the image of the arboreal representation is the fiber-crossed product of some I-pair (L, R, θ), with $L \subseteq E[\ell^n]$ and $R \subseteq G_{T_n/F}$. Since we are looking for subgroups of $E[\ell^n] \rtimes G_{T_n/F}$ that project surjectively onto the second factor, $R = G_{T_n/F}$. It is easy to see that condition (i) in Definition 2.9 implies $\theta(1) \in L$, so that

$$\begin{aligned} L &\cong \{(u, 1) : u \in L\} \\ &\cong \{(\kappa_n(\sigma), 1) : \sigma\big|_{E[\ell^n]} = 1\} \\ &\cong \{\kappa_n(\sigma) : \sigma \in G_{K_n/T_n}\} \\ &\cong \mathrm{im}\kappa_n. \end{aligned}$$

It follows that the possible images of the nth Kummer map are precisely the possible subgroups L of $E[\ell^n]$ that form an I-pair with $R = G_{T_n/F}$. To find the possible images of the arboreal representation, we therefore want to find all subgroups L and all maps θ satisfying conditions (i) and (ii) in Definition 2.9. We begin with the former task by focusing on condition (ii), which, because our group $U = E[\ell^n]$ is abelian, becomes:

(ii') $\qquad M.a \in L$ for all $M \in G_{T_n/F}$ and for all $a \in L$.

We therefore first seek all $G_{T_n/F}$-invariant subspaces L of $E[\ell^n]$. Using Proposition 3.2, we have that one of the following holds:

(1) $L = E[\ell^n]$

(2) $L = \left\langle \binom{1}{0}, \binom{0}{\ell} \right\rangle$

(3) $L \subseteq E[\ell^{n-1}] = \left\langle \binom{\ell}{0}, \binom{0}{\ell} \right\rangle$.

We now prove Theorem 3.4.

Proof of Theorem 3.4. From Proposition 3.3, under the hypothesis $\alpha \notin E(F) \cap \ell E(T_n)$, to determine $\mathrm{im}\omega_n$ it suffices to consider cases (1) and (2) above. Recall that in both cases $R = G_{T_n/F}$. It is clear that if we are in case (1), so that $L = E[\ell^n]$, then for any map θ we have $L \rtimes_{\varphi,\theta} R$ is the full group $E[\ell^n] \rtimes G_{T_n/F}$.

We are left then to consider the case where $L = \left\langle \binom{1}{0}, \binom{0}{\ell} \right\rangle$. We want to find all maps $\theta : G_{T_n/F} \to E[\ell^n]$ so that $(L, G_{T_n/F}, \theta)$ is an I-pair for $E[\ell^n] \rtimes G_{T_n/F}$. By condition (i) in Definition 2.9, this is equivalent to finding all such maps θ satisfying $\theta(MN) - \theta(M) - M.\theta(N) \in L$ for all $M, N \in G_{T_n/F}$. Recall that given θ, the subgroup we obtain is the fiber-crossed product $\{(a + \theta(M), M) : a \in L,\ M \in G_{T_n/F}\}$. Since we are only interested in the distinct possible subgroups and we have that two I-pairs (L, R, θ) and (L', R', θ') give the same subgroup if and only if $L = L'$, $R = R'$, and $\theta(M) - \theta'(M) \in L$ for all $M \in R$, it is enough to find all maps $\theta : G_{T_n/F} \to E[\ell^n]/L \cong \mathbb{Z}/\ell$ such that for all $M, N \in G_{T_n/F}$ we have $\theta(MN) \equiv \theta(M) + M \cdot \theta(N) \pmod{\ell}$. Here, the action of $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_{T_n/F}$ on $\mathbb{Z}/\ell$ is multiplication by d. Our condition can therefore be restated as

$$\theta\left(\begin{smallmatrix} ar+bt & as+bu \\ cr+dt & cs+du \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) + d\theta\left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right) \pmod{\ell} \tag{3.1}$$

where $a, r \equiv 1 \pmod{\ell}$, $c, t \equiv 0 \pmod{\ell}$, and d, u are units.

To find all possible θ we now enumerate specific choices for M and N to determine necessary conditions θ must satisfy. We will make our choices of $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} r & s \\ t & u \end{smallmatrix}\right)$ clear by always writing our statements in the form of (3.1).

1. $\theta\left(\begin{smallmatrix} x_1x_2 & 0 \\ 0 & 1 \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} x_1 & 0 \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} x_2 & 0 \\ 0 & 1 \end{smallmatrix}\right)$

2. $\theta\left(\begin{smallmatrix} 1 & y_1+y_2 \\ 0 & 1 \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & y_1 \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & y_2 \\ 0 & 1 \end{smallmatrix}\right)$

3. $\theta\left(\begin{smallmatrix} 1 & 0 \\ z_1+z_2 & 1 \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z_1 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ z_2 & 1 \end{smallmatrix}\right)$

4. $\theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w_1w_2 \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w_1 \end{smallmatrix}\right) + w_1\theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w_2 \end{smallmatrix}\right)$

Capitalizing on the fact that $M = \left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$ and $N = \left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$ commute, we obtain

5. $\theta\left(\begin{smallmatrix} x & 0 \\ 0 & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$

6. $\theta\left(\begin{smallmatrix} x & 0 \\ 0 & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$

Note that (5) and (6) give us that $\theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) \equiv w\theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right)$ for all x and w, so since $\ell \neq 2$ we have

7. $\theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) \equiv 0$ for all x

8. $\theta\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} x & 0 \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & y/x \\ z & w \end{smallmatrix}\right)$
$\equiv \theta\left(\begin{smallmatrix} 1 & y/x \\ z & w \end{smallmatrix}\right)$ by (7)

It is therefore enough to determine $\theta\left(\begin{smallmatrix} 1 & y \\ z & w \end{smallmatrix}\right)$ for all y, z, w.

9. $\theta\left(\begin{smallmatrix} 1 & y \\ z & 1 \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1-yz & 0 \\ z & 1 \end{smallmatrix}\right)$
$\equiv \theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right)$ by (8)

10. $\theta\left(\begin{smallmatrix} 1 & y \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} 1 & y \\ z/w & 1 \end{smallmatrix}\right)$
$\equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} 1 & 0 \\ z/w & 1 \end{smallmatrix}\right)$ by (9)
$\equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right)$ by (3)

11. $\theta\left(\begin{smallmatrix} 1 & y \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & y/w \\ z & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$
$\equiv \theta\left(\begin{smallmatrix} 1 & y/w \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$ by (9)
$\equiv \dfrac{1}{w}\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$ by (2)

Note that (10) and (11) give $\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \equiv w^2\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$ for all y, w. Since $\ell > 3$, we have

12. $\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right) \equiv 0$ for all y

13. $\theta\left(\begin{smallmatrix} 1 & y \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z & w \end{smallmatrix}\right) + w\theta\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)$
$\equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z & w \end{smallmatrix}\right)$ by (12)

14. $\theta\left(\begin{smallmatrix} 1 & 0 \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$

15. $\theta\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \equiv \theta\left(\begin{smallmatrix} 1 & y/x \\ z & w \end{smallmatrix}\right)$ by (8)
$\equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z & w \end{smallmatrix}\right)$ by (13)
$\equiv \theta\left(\begin{smallmatrix} 1 & 0 \\ z & 1 \end{smallmatrix}\right) + \theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$ by (14)

Note that any θ satisfying conditions (3), (4), and (15) is determined by $\theta\left(\begin{smallmatrix} 1 & 0 \\ \ell & 1 \end{smallmatrix}\right)$ and $\theta\left(\begin{smallmatrix} 1 & 0 \\ 0 & d \end{smallmatrix}\right)$, where d is a fixed generator of $(\mathbb{Z}/\ell^n)^\times$. Condition (3) gives us that $\theta\left(\begin{smallmatrix} 1 & 0 \\ c\ell & 1 \end{smallmatrix}\right) \equiv c\theta\left(\begin{smallmatrix} 1 & 0 \\ \ell & 1 \end{smallmatrix}\right)$ and

condition (4) together with a quick induction argument gives us that $\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d^m\end{smallmatrix}\right) \equiv (d^{m-1} + \ldots + d + 1)\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right)$. Indeed,

$$\begin{aligned}\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d^m\end{smallmatrix}\right) &\equiv \theta\left(\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right)^m\right)\\ &\equiv \theta\left(\begin{smallmatrix}1 & 0\\ 0 & d^{m-1}\end{smallmatrix}\right) + d^{m-1}\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right)\\ &\equiv (d^{m-1} + \ldots + d + 1)\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right).\end{aligned}$$

We now show that any θ meeting conditions (3), (4), and (15) above satisfies (3.1). Let $\theta\left(\begin{smallmatrix}1 & 0\\ \ell & 1\end{smallmatrix}\right) \equiv \gamma_1$ and $\theta\left(\begin{smallmatrix}1 & 0\\ 0 & d\end{smallmatrix}\right) \equiv \gamma_2'$, where $\gamma_1, \gamma_2' \in \mathbb{Z}/\ell$. On the one hand, we have

$$\begin{aligned}\theta\left(\begin{smallmatrix}a & b\\ \ell c & d^m\end{smallmatrix}\right) + d^m\theta\left(\begin{smallmatrix}r & s\\ \ell t & d^n\end{smallmatrix}\right) &\equiv \theta\left(\begin{smallmatrix}1 & 0\\ \ell c & 1\end{smallmatrix}\right) + \theta\left(\begin{smallmatrix}1 & 0\\ 0 & d^m\end{smallmatrix}\right) + d^m(\theta\left(\begin{smallmatrix}1 & 0\\ \ell t & 1\end{smallmatrix}\right) + \theta\left(\begin{smallmatrix}1 & 0\\ 0 & d^n\end{smallmatrix}\right)\\ &\equiv c\gamma_1 + (d^{m-1} + \ldots + d + 1)\gamma_2' + d^m(t\gamma_1 + (d^{n-1} + \ldots + d + 1)\gamma_2')\\ &\equiv (c + d^m t)\gamma_1 + (d^{m+n-1} + \ldots + d + 1)\gamma_2'.\end{aligned}$$

On the other hand, we have

$$\begin{aligned}\theta\left(\begin{smallmatrix}ar+\ell bt & as+bd^n\\ \ell(cr+d^m t) & \ell cs+d^{m+n}\end{smallmatrix}\right) &\equiv \theta\left(\begin{smallmatrix}1 & 0\\ \ell(cr+d^m t) & 1\end{smallmatrix}\right) + \theta\left(\begin{smallmatrix}1 & 0\\ 0 & \ell cs+d^{m+n}\end{smallmatrix}\right)\\ &\equiv (cr + d^m t)\gamma_1 + (d^{k-1} + \ldots + d + 1)\gamma_2',\end{aligned}$$

where we let $d^k = \ell cs + d^{m+n}$. Since $r \equiv 1 (\text{mod } \ell)$ and $d^k \equiv d^{m+n} (\text{mod } \ell)$, we have

$$\begin{aligned}\theta\left(\begin{smallmatrix}ar+\ell bt & as+bd^n\\ \ell(cr+d^m t) & \ell cs+d^{m+n}\end{smallmatrix}\right) &\equiv (c + d^m t)\gamma_1 + \frac{d^k - 1}{d-1}\gamma_2'\\ &\equiv (c + d^m t)\gamma_1 + \frac{d^{m+n} - 1}{d-1}\gamma_2'.\\ &\equiv (c + d^m t)\gamma_1 + (d^{m+n-1} + \ldots + d + 1)\gamma_2'\end{aligned}$$

It follows that θ satisfies condition (3.1). Letting $\gamma_2 = \frac{\gamma_2'}{d-1}$, we obtain the subgroup

$$\left\{\left(u + \left(\begin{smallmatrix}0\\ c_1(M)\gamma_1 + (d_0(M)-1)\gamma_2\end{smallmatrix}\right), M\right) : u \in L, M \in G_{T_n/F}\right\} \subseteq E[\ell^n] \rtimes G_{T_n/F}.$$

It is clear that each pair (γ_1, γ_2) gives a different subgroup, since two pairs give the same subgroup if and only if $z\gamma_1 + (w-1)\gamma_2 \equiv z\tilde{\gamma_1} + (w-1)\tilde{\gamma_2} \pmod{\ell}$ for all $z \in \mathbb{Z}/\ell$ and $w \in (\mathbb{Z}/\ell)^\times$, which occurs if and only if $(\gamma_1, \gamma_2) = (\tilde{\gamma_1}, \tilde{\gamma_2})$. Our result now follows.

□

The hypothesis in Theorem 3.4 imposes a condition on α for each $n \geq 1$. The following shows that it is enough to verify this condition for $n = 2$ only.

Proposition 3.5. *Let $G_{T_n/F}$ be as above. Then $E(F) \cap \ell E(T_n) = E(F) \cap \ell E(T_{n+1})$ for all $n \geq 2$.*

Proof. Inclusion from left to right is clear. To prove the reverse inclusion, let $\alpha \in E(F) \cap \ell E(T_{n+1})$. Then $\beta_1 \in E(T_{n+1})$. We want to show $\beta_1 \in E(T_n)$. Consider the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 0 & \longrightarrow & H^1(G_{T_n/F}, E[\ell]) & \xrightarrow{\inf} & H^1(G_{\bar{\mathbb{Q}}/F}, E[\ell]) & \xrightarrow{\text{res}} & H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell]) \\ & & \downarrow{\scriptstyle \inf} & & \| & & \downarrow{\scriptstyle \text{res}} \\ 0 & \longrightarrow & H^1(G_{T_{n+1}/F}, E[\ell]) & \xrightarrow{\inf} & H^1(G_{\bar{\mathbb{Q}}/F}, E[\ell]) & \xrightarrow{\text{res}} & H^1(G_{\bar{\mathbb{Q}}/T_{n+1}}, E[\ell]). \end{array}$$

We see then that it is enough to show that the inflation map

$$H^1(G_{T_n/F}, E[\ell]) \longrightarrow H^1(G_{T_{n+1}/F}, E[\ell])$$

is an isomorphism. Indeed, if it were an isomorphism, then since the co-chain $\sigma(\beta_1) - \beta_1$ in $H^1(G_{\bar{\mathbb{Q}}/F}, E[\ell])$ restricted to $H^1(G_{\bar{\mathbb{Q}}/T_{n+1}}, E[\ell])$ is zero, following the diagram, we would have it is also zero restricted to $H^1(G_{\bar{\mathbb{Q}}/T_n}, E[\ell])$, so that $\beta_1 \in E(T_n)$.

To prove this isomorphism, we show the inflation maps

$$H^1(G_{T_n/F}, \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle) \longrightarrow H^1(G_{T_{n+1}/F}, \langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle)$$

and

$$H^1(G_{T_n/F}, E[\ell]/\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle) \longrightarrow H^1(G_{T_{n+1}/F}, E[\ell]/\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle)$$

are both isomorphisms. We first show the latter is an isomorphism. Note that any co-chain $\xi \in H^1(G_{T_m/F}, E[\ell]/\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle)$ satisfies $\xi(MN) = \xi(M) + M.\xi(N)$ for all M and N in $G_{T_m/F}$. Since M acts by multiplication by $d(M)$ and $E[\ell]/\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right) \rangle \cong \mathbb{Z}/\ell$, the cochain condition is equivalent to

$$\xi(MN) \equiv \xi(M) + d(M)\xi(N) \pmod{\ell}.$$

But this is exactly the condition that arose in the proof of 3.4. Thus for $n \geq 2$, $\xi(M) = \left(\begin{smallmatrix} 0 \\ c_1(M)\gamma_1 + (d_0(M)-1)\gamma_2 \end{smallmatrix}\right)$ for some $\gamma_1, \gamma_2 \in \mathbb{Z}/\ell$. Since $M.\left(\begin{smallmatrix} 0 \\ \gamma_2 \end{smallmatrix}\right) - \left(\begin{smallmatrix} 0 \\ \gamma_2 \end{smallmatrix}\right) \equiv \left(\begin{smallmatrix} 0 \\ (d_0(M)-1)\gamma_2 \end{smallmatrix}\right) \pmod{\ell}$ is

a coboundary, we conclude $H^1(G_{T_n/F}, E[\ell]/\langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) \cong H^1(G_{T_{n+1}/F}, E[\ell]/\langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) \cong \mathbb{Z}/\ell$ for all $n \geq 2$.

To show that $H^1(G_{T_n/F}, \langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) \cong H^1(G_{T_{n+1}/F}, \langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle)$, we prove the following lemma.

Lemma 3.6. *Let H_m be the determinant one subgroup of $G_{T_m/F}$. Then $H_m = [G_{T_m/F}, G_{T_m/F}]$, the commutator subgroup of $G_{T_m/F}$.*

Proof. It is clear that $[G_{T_m/F}, G_{T_m/F}] \subseteq H_m$. To show reverse containment, let $M \in H_m$. Then M is of the form $M = \left(\begin{smallmatrix} a & b \\ c & \frac{1+bc}{a} \end{smallmatrix}\right)$, $a \equiv 1 \pmod{\ell}$, $c \equiv 0 \pmod{\ell}$. Note that

$$M = \left(\begin{smallmatrix} 1 & 0 \\ \frac{c}{a} & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & -a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \frac{1}{1-a} & 0 \\ 1 & \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & 0 \\ a-1 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & \frac{b}{a} \\ 0 & 1 \end{smallmatrix}\right).$$

It follows that H_m is generated by $E_1 = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $E_2 = \left(\begin{smallmatrix} 1 & 0 \\ \ell & 1 \end{smallmatrix}\right)$. It is therefore enough to show E_1 and E_2 are in $[G_{T_m/F}, G_{T_m/F}]$. Indeed, letting $A = \left(\begin{smallmatrix} 2 & 0 \\ 0 & \frac{1}{2} \end{smallmatrix}\right)$, $B_1 = \left(\begin{smallmatrix} 1 & \frac{1}{3} \\ 0 & 1 \end{smallmatrix}\right)$, and $B_2 = \left(\begin{smallmatrix} 1 & \\ -\frac{4}{3}\ell & 0 \\ & 1 \end{smallmatrix}\right)$, we have

$$E_1 = AB_1A^{-1}B_1^{-1}$$

and

$$E_2 = AB_2A^{-1}B_2^{-1}.$$

□

Since $G_{T_m/F}$ acts trivially on $\langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle$ for all m, we have that

$$H^1(G_{T_m/F}, \langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) = \mathrm{Hom}(G_{T_m/F}, \mathbb{Z}/\ell).$$

By Lemma 3.6, $H_m = [G_{T_m/F}, G_{T_m/F}]$, so any homomorphism $G_{T_m/F} \to \mathbb{Z}/\ell$ maps H_m to zero. We are therefore reduced to finding all homomorphisms $\mathrm{Hom}(G_{T_m/F}/H_m, \mathbb{Z}/\ell)$. Since $G_{T_m/F}/H_m \cong (\mathbb{Z}/\ell^m)^\times$, which is cyclic of order $\ell^{m-1}(\ell-1)$, we have for $m \geq 2$ that

$$H^1(G_{T_m/F}, \langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) \cong \mathbb{Z}/\ell.$$

Since $(E[\ell]/\langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle)^{G_{T_m/F}} = 0$ we may consider the exact sequence

$$0 \longrightarrow H^1(G_{T_m/F}, \langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle) \longrightarrow H^1(G_{T_m/F}, E[\ell]) \longrightarrow H^1(G_{T_m/F}, E[\ell]/\langle \left(\begin{smallmatrix}1\\0\end{smallmatrix}\right)\rangle).$$

Noting that $\xi_1 : M \mapsto \left(\begin{smallmatrix} a_1(M) \\ c_1(M) \end{smallmatrix}\right)$ and $\xi_2 : M \mapsto \left(\begin{smallmatrix} \log(\det(M)) \\ 0 \end{smallmatrix}\right)$ are distinct nonzero elements of $H^1(G_{T_m/F}, E[\ell])$, we conclude $H^1(G_{T_m/F}, E[\ell]) \cong (\mathbb{Z}/\ell)^2$ for all $m \geq 2$. □

3.3 The Density Computation for Type I Reducible Elliptic Curves

We now compute $\mathcal{F}(G)$ in each of the cases from Proposition 3.4. We begin with case (i).

Proposition 3.7. *Suppose we are in case (i) in Theorem 3.4. Then* $\mathcal{F}(G) = \frac{\ell^3-\ell-1}{\ell^4+\ell^3-\ell-1}$.

Proof. Recall that

$$\mathcal{F}(G) = \lim_{n\to\infty} \frac{\#\{\sigma \in G_{K_n/F} : \sigma(\beta) = \beta \text{ for some } \beta \in [\ell^n]^{-1}(\alpha)\}}{\#G_{K_n/F}}$$

From Proposition 2.4, the numerator above is equal to $\#\{(v, M) \in \mathrm{im}\omega_n : v \in \mathrm{im}(M-I)\}$. Since the image of a matrix X with $\det(X) \neq 0$ has index $\ell^{\mathrm{ord}_\ell(\det(X))}$, we have that

$$\begin{aligned}\mathcal{F}(G) &= \lim_{n\to\infty} \frac{\sum_{M\in G_{T_n/F}} \#\mathrm{im}(M-I)}{\#G_{T_n/F}\cdot\ell^{2n}} \\ &= \lim_{n\to\infty} \frac{\sum' \ell^{-\mathrm{ord}_\ell(\det(M-I))}}{\#G_{T_n/F}} + \frac{\sum'' \#\mathrm{im}(M-I)}{\#G_{T_n/F}\cdot\ell^{2n}},\end{aligned}$$

where $\sum'$ and $\sum''$ are taken over all $M \in G_{T_n/F}$ with $\det(M-I) \not\equiv 0 \pmod{\ell^n}$ and $\det(M-I) \equiv 0 \pmod{\ell^n}$, respectively. Since the second sum goes to zero as $n \to \infty$, we have that

$$\mathcal{F}(G) = \sum_{n=1}^{\infty} \frac{s_n}{\ell^{n-1}\#G_{T_n/F}},$$

where $s_n = \#\{M \in G_{T_n/F} : \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n}\}$.

Since $M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}$, we may write $M-I = \left(\begin{smallmatrix} x\ell & y \\ z\ell & w \end{smallmatrix}\right)$, where $x, z \in \mathbb{Z}/\ell^{n-1}$ and $y, w \in \mathbb{Z}/\ell^n$ such that $w \not\equiv -1 \pmod{\ell}$. Then $s_1 = 0$ and for $n \geq 2$,

$$s_n = \#\{(x, y, z, w) \in \mathbb{Z}/\ell^{n-1} \times \mathbb{Z}/\ell^n \times \mathbb{Z}/\ell^{n-1} \times \mathbb{Z}/\ell^n : w \not\equiv -1 \pmod{\ell}, \mathrm{ord}_\ell(xw - yz) = n-2\}.$$

To compute s_n we use the following lemma.

Lemma 3.8. *Define*

$$r_n = \#\{(a, b, c, d) \in (\mathbb{Z}/\ell^n)^4 : ad - bc \equiv t\ell^{n-1} \pmod{\ell^n}, t \in (\mathbb{Z}/\ell)^\times\}.$$

Then r_n satisfies the recursive relation

$$r_n = \ell^{3n-3}(\ell^2-1)^2 + \ell^4 r_{n-2},$$

where $r_1 = \ell(\ell-1)(\ell^2-1)$ and we define $r_0 = 0$.

Proof. Note that r_1 is simply $\#\mathrm{GL}_2(\mathbb{Z}/\ell)$, which is $\ell(\ell-1)(\ell^2-1)$. We now find r_n for $n \geq 2$. Suppose first that $a \in \mathbb{Z}/\ell^n$ is a unit. Then $d \equiv (t\ell^{n-1}+bc)a^{-1}$ is completely determined (mod ℓ^n). There are thus $\ell^{3n-1}(\ell-1)^2$ tuples in this case. Now suppose a is not a unit, but b is. Then $c \equiv (ad - t\ell^{n-1})b^{-1}$ is completely determined (mod ℓ^n). There are thus $\ell^{3n-2}(\ell-1)^2$ tuples in this case. Now assume a and b are not units, but c is a unit. Note that in this case, any choice of non-unit for a forces b to be a non-unit. We have then that $b \equiv (ad - t\ell^{n-1})c^{-1}$ is completely determined (mod ℓ^n) and we are free to choose a (non-unit), c (unit), and d (anything). There are therefore $\ell^{3n-2}(\ell-1)^2$ tuples in this case. Next, suppose a, b, and c are not units, but d is a unit. Note that in this case, any choice of non-unit for b forces a to also be a non-unit. We have then that $a \equiv (t\ell^{n-1}+bc)d^{-1}$ is completely determined (mod ℓ^n) and we are free to choose b (non-unit), c (non-unit), and d (unit). There are therefore $\ell^{3n-3}(\ell-1)^2$ tuples in this case. If $n=2$ and a,b,c,d are all non-units, then $ad-bc \equiv 0 \not\equiv t\ell$ (mod ℓ^2), $t \in (\mathbb{Z}/\ell)^\times$. This therefore exhausts all possibilities for $n=2$, so we have $r_2 = \ell^3(\ell^2-1)$, which satisfies the desired recursion if we set $r_0 = 0$.

Assume now that $n \geq 3$ and that all of a, b, c, and d are not units. Then we can write $a = a'\ell$, $b = b'\ell$, $c = c'\ell$, and $d = d'\ell$, where $a', b', c', d' \in \mathbb{Z}/\ell^{n-1}$. Since $ad - bc \equiv (a'd' - b'c')\ell^2$, we therefore seek to count

$$\#\{(a',b',c',d') \in (\mathbb{Z}/\ell^{n-1})^4 : a'd' - b'c' \equiv t\ell^{n-3} \pmod{\ell^{n-2}}, t \in (\mathbb{Z}/\ell)^\times\}.$$

Note that since our imposed condition is (mod ℓ^{n-2}), the above quantity is equal to

$$\ell^4 \cdot \#\{(a',b',c',d') \in (\mathbb{Z}/\ell^{n-2})^4 : a'd' - b'c' \equiv t\ell^{n-3} \pmod{\ell^{n-2}}, t \in (\mathbb{Z}/\ell)^\times\}.$$

Since this is $\ell^4 r_{n-2}$, our result follows. □

We now compute s_n. First suppose w is a unit. Then x is completely determined, so we have $\ell^{3n-2}(\ell-1)(\ell-2)$ matrices in this case.

Next, suppose w is not a unit, but y is a unit. Then z is completely determined, so that there are $\ell^{3n-3}(\ell-1)^2$ matrices in this case. Note this exhausts all cases for $n=2$.

Finally, assume $n \geq 2$ and suppose both y and w are not units. Then setting $y = y'\ell$ and $w = w'\ell$ with $y', w' \in \mathbb{Z}/\ell^{n-1}$, we see that the number of matrices in this case is $\#\{(x,y',z,w') \in (\mathbb{Z}/\ell^{n-1})^4 : xw' - y'z \equiv t\ell^{n-3} \pmod{\ell^{n-2}}, t \in (\mathbb{Z}/\ell)^\times\} = \ell^4 r_{n-2}$.

We have then that $s_n = \ell^{3m-3}(\ell-1)(\ell^2-\ell-1) + \ell^4 r_{n-2}$ so that

$$\begin{aligned}\mathcal{F}(G) &= \sum_{n=2}^{\infty} \frac{s_n}{\ell^{n-1}\#G_{T_n/F}} \\ &= \sum_{n=2}^{\infty} \frac{\ell^{3n-3}(\ell-1)(\ell^2-\ell-1)}{\ell^{5n-4}(\ell-1)} + \sum_{n=3}^{\infty} \frac{\ell^4 r_{n-2}}{\ell^{5n-4}(\ell-1)}\end{aligned}$$

Now, the first sum is a geometric series and sums to $\frac{\ell^2-\ell-1}{\ell(\ell^2-1)}$. To find the second sum, which we denote by S, we use Lemma 3.8 and obtain

$$S = \sum_{n=3}^{\infty} \frac{r_n - \ell^{3n-3}(\ell^2-1)^2}{\ell^{5n-4}(\ell-1)}.$$

Splitting this into two sums, we see that the second is geometric and sums to $-\frac{\ell+1}{\ell^3}$ and the first, after reindexing and some manipulation, is $\ell^6 S - \frac{\ell^4 r_1}{\ell^5(\ell-1)} - \frac{\ell^4 r_2}{\ell^1 0(\ell-1)}$. Using $r_1 = \ell(\ell-1)^2(\ell+1)$ and $r_2 = \ell^3(\ell^2-1)^2$, we can solve for S to obtain $S = \frac{1}{\ell(\ell^3-1)}$. We conclude that

$$\mathcal{F}(G) = \frac{\ell^3-\ell-1}{\ell^4+\ell^3-\ell-1}$$

as desired. □

We now compute $\mathcal{F}(G)$ in case (ii). We will have to consider the subcases $\gamma_1 \equiv 0 \pmod{\ell}$ and $\gamma_1 \not\equiv 0 \pmod{\ell}$.

Proposition 3.9. *Suppose we are in case (ii) of Theorem 3.4. Then* $\mathcal{F}(G) = \frac{2\ell^3-\ell^2-2}{\ell^4+\ell^3-\ell-1}$ *if* $\gamma_1 \equiv 0 \pmod{\ell}$ *and* $\mathcal{F}(G) = \frac{\ell^3-\ell^2-1}{\ell^4+\ell^3-\ell-1}$ *if* $\gamma_1 \not\equiv 0 \pmod{\ell}$.

Proof. From above, we know that

$$\mathcal{F}(G) = \lim_{n\to\infty} \frac{\#\{(v,M) \in \mathrm{im}(\omega_n) : v \in \mathrm{im}(M-I)}{\#\mathrm{im}(\omega_n)\}.$$

Since we are in case (ii), for M of the form $\left(\begin{smallmatrix} 1+x\ell & y \\ z\ell & w \end{smallmatrix}\right)$ with $w \not\equiv 0 \pmod{\ell}$, we have that $v \equiv \left(\begin{smallmatrix} * \\ z\gamma_1+(w-1)\gamma_2 \end{smallmatrix}\right) \pmod{\ell}$.

First suppose $w \not\equiv 1 \pmod{\ell}$. We have that $v \in \mathrm{im}(M-I)$ if and only if v is in the column space of $M-I$, which is true if and only if

$$a = \epsilon_1 \left(\begin{smallmatrix} x\ell \\ z\ell \end{smallmatrix}\right) + \epsilon_2 \left(\begin{smallmatrix} y \\ w-1 \end{smallmatrix}\right).$$

Since $w-1$ is a unit, we have that $\epsilon_2 \equiv \frac{z\gamma_1}{w-1} + \gamma_2 \pmod{\ell}$. We therefore want to determine the number of elements in the set

$$\left\{\epsilon_1 \left(\begin{smallmatrix} x\ell \\ z\ell \end{smallmatrix}\right) + \epsilon_2' \ell \left(\begin{smallmatrix} y \\ w-1 \end{smallmatrix}\right) + \left(\begin{smallmatrix} 0 \\ z_1\gamma_1+(w_0-1)\gamma_2 \end{smallmatrix}\right) \in (\mathbb{Z}/\ell^n)^2 : z \equiv z_1 \pmod{\ell^2} \text{ and } w \equiv w_0 \not\equiv 0 \pmod{\ell}\right\}.$$

But this is the same as the size of the column space of the matrix $M' = \left(\begin{smallmatrix} x & y \\ z & w-1 \end{smallmatrix}\right) \in \mathrm{GL}_2(\mathbb{Z}/\ell^{n-1})$, which is $\ell^{(2n-2)-\mathrm{ord}_\ell(\det(M'-I))}$. Since $\mathrm{ord}_\ell(\det(M'-I)) = \mathrm{ord}_\ell(\det(M-I)) - 1$, we conclude the number of pairs $(v, M) \in \mathrm{im}\omega_n$ for fixed $M \in G_{T_n/F}$ satisfying $d_0(M) \not\equiv 1 \pmod{\ell}$ is $\ell^{2n-\mathrm{ord}_\ell(\det(M-I))-1}$.

Now suppose $w \equiv 1 \pmod{\ell}$. Then for v to be in the image of $M - I$, it must be that $v \equiv \left(\begin{smallmatrix} * \\ 0 \end{smallmatrix}\right) \pmod{\ell}$. On the other hand, since $v \equiv \left(\begin{smallmatrix} * \\ z\gamma_1 + (w-1)\gamma_2 \end{smallmatrix}\right)$, we conclude $z\gamma_1 \equiv 0 \pmod{\ell}$. For any $v \in \mathrm{im}(M-I)$, we have then that $(v, M) \in \mathrm{im}\omega_n$. It follows that for fixed $M \in G_{T_n/F}$ satisfying $w \equiv 1 \pmod{\ell}$, the number of pairs (v, M) in the image of ω_n is $\#\mathrm{im}(M-I) = \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}$.

We can now split $\mathcal{F}(G)$ into two sums.

$$\begin{aligned}
\mathcal{F}(G) &= \lim_{n\to\infty} \frac{\#\{(v,M) \in \mathrm{im}\omega_n : v \in \mathrm{im}(M-I), d_0(M) \not\equiv 1\}}{\#\mathrm{im}\omega_n} \\
&\quad + \lim_{n\to\infty} \frac{\#\{(v,M) \in \mathrm{im}\omega_n : v \in \mathrm{im}(M-I), d_0(M) \equiv 1\}}{\#\mathrm{im}\omega_n} \\
&= \lim_{n\to\infty} \frac{\sum\limits_{\substack{M \in G_{T_n/F} \\ d_0(M) \not\equiv 1}} \ell^{2n-\mathrm{ord}_\ell(\det(M-I))-1}}{\#G_{T_n/F}\ell^{2n-1}} + \lim_{n\to\infty} \frac{\sum\limits_{\substack{M \in G_{T_n/F} \\ d_0(M) \equiv 1}} \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}}{\#G_{T_n/F}\ell^{2n-1}} \\
&= \sum_{m=1}^{\infty} \frac{s'_m}{\#G_{T_m/F}\ell^{m-1}} + \sum_{m=1}^{\infty} \frac{s''_m}{\#G_{T_m/F}\ell^{m-2}}
\end{aligned}$$

where

$$s'_m = \#\left\{ M \in G_{T_m/F} : \begin{array}{l} d_0(M) \not\equiv 1 \pmod{\ell}, \\ \det(M-I) \equiv 0 \pmod{\ell^{m-1}}, \text{but } \not\equiv 0 \pmod{\ell^m} \end{array} \right\}$$

and

$$s''_m = \#\left\{ M \in G_{T_m/F} : \begin{array}{l} d_0(M) \equiv 1 \pmod{\ell}, \\ \det(M-I) \equiv 0 \pmod{\ell^{m-1}}, \text{but } \not\equiv 0 \pmod{\ell^m} \end{array} \right\}.$$

Note that $s'_1 = 0$ and that for $m \geq 2$,

$$s'_m = \#\Big\{ (x,y,z,w,t) \in \mathbb{Z}/\ell^{m-1} \times \mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^{m-1} \times (\mathbb{Z}/\ell^m)^\times \times (\mathbb{Z}/\ell)^\times : \\ w \not\equiv 1 \pmod{\ell},\ x(w-1)\ell - yz\ell \equiv t\ell^{m-1} \pmod{\ell^m} \Big\}.$$

The second condition is equivalent to $x(w-1) - yz \equiv t\ell^{m-2} \pmod{\ell^{m-1}}$, which, since $w-1$ is a unit, means x is completely determined. Since we are free to choose y, z, w, and t, we have that $s'_m = \ell^{3m-2}(\ell-1)(\ell-2)$ for all $m \geq 2$. Using that $\#G_{T_m/F} = \ell^{4m-3}(\ell-1)$, we can now compute

the first sum as a geometric series:

$$\sum_{m=1}^{\infty} \frac{s'_m}{\#G_{T_m/F}\ell^{m-1}} = \sum_{m=2}^{\infty} \frac{\ell-2}{\ell^{2m-2}} = \frac{\ell-2}{\ell^2-1}.$$

Recall that for the second sum, we are in the situation where $\gamma_1 c_1(M) \equiv 0 \pmod{\ell}$, meaning $\gamma_1 \equiv 0 \pmod{\ell}$ or $c_1(M) \equiv 0 \pmod{\ell}$. If $\gamma_1 \equiv 0$, then writing $M - I = \left(\begin{smallmatrix} x\ell & y \\ z\ell & w\ell \end{smallmatrix}\right)$, we see that $s''_1 = 0$ and for $m \geq 2$

$$s''_m = \#\Bigg\{(x,y,z,w,t) \in \mathbb{Z}/\ell^{m-1} \times \mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^{m-1} \times \mathbb{Z}/\ell^{m-1} \times (\mathbb{Z}/\ell)^\times : \\ xw\ell^2 - yz\ell \equiv t\ell^{m-1} \pmod{\ell^m}\Bigg\}.$$

If y is a unit, then the above condition is equivalent to $xw\ell - yz \equiv t\ell^{m-2} \pmod{\ell^{m-1}}$, which means z is completely determined. This gives $\ell^{3m-3}(\ell-1)^2$ tuples in this case.

This exhausts the possibilities for $m = 2$, so let $m \geq 3$. If y is a nonunit, setting $y = y'\ell$, $y' \in \mathbb{Z}/\ell^{m-1}$, the above condition then becomes $xw - yz \equiv t\ell^{m-3} \pmod{\ell^{m-2}}$. Using the quantity r_n defined in Lemma 3.8, we see that the number of tuples in this case is $\ell^4 r_{m-2}$.

We can now compute the second sum to be

$$\begin{aligned}\sum_{m=1}^{\infty} \frac{s''_m}{\#G_{T_m/F}\ell^{m-2}} &= \sum_{m=2}^{\infty} \frac{\ell-1}{\ell^{2m-2}} + \frac{\ell}{\ell-1} \sum_{m=3}^{\infty} \frac{r_{m-2}}{\ell^{5m-8}} \\ &= \frac{\ell-1}{\ell^2-1} + \frac{1}{\ell^3-1}.\end{aligned}$$

We conclude for case (ii) with $\gamma \equiv 0 \pmod{\ell}$ that $\mathcal{F}(G) = \frac{\ell-2}{\ell^2-1} + \frac{\ell-1}{\ell^2-1} + \frac{1}{\ell^3-1} = \frac{2\ell^3-\ell^2-2}{\ell^4+\ell^3-\ell-1}$, as claimed.

If $\gamma_1 \not\equiv 0 \pmod{\ell}$, then $c_1(M) \equiv 0 \pmod{\ell}$, so we are only considering matrices M such that $M - I$ is of the form $\left(\begin{smallmatrix} x\ell & y \\ z'\ell^2 & w\ell \end{smallmatrix}\right)$. We have then that $s''_1 = s''_2 = 0$ and for $m \geq 3$,

$$s''_m = \#\Bigg\{(x,y,z',w,t) \in \mathbb{Z}/\ell^{m-1} \times \mathbb{Z}/\ell^m \times \mathbb{Z}/\ell^{m-2} \times \mathbb{Z}/\ell^{m-1} \times (\mathbb{Z}/\ell)^\times : \\ xw\ell^2 - yz'\ell^2 \equiv t\ell^{m-1} \pmod{\ell^m}\Bigg\}.$$

The above condition is equivalent to $xw - yz' \equiv t\ell^{m-3} \pmod{\ell^{m-2}}$. There are $\ell^4 r_{m-2}$ tuples in this case. Our second sum can then be computed to be

$$\sum_{m=1}^{\infty} \frac{s''_m}{\#G_{T_m/F}\ell^{m-2}} = \frac{\ell}{\ell-1} \sum_{m=3}^{\infty} \frac{r_{m-2}}{\ell^{5m-8}} = \frac{1}{\ell^3-1}.$$

We thus have for case (ii) with $\gamma_1 \not\equiv 0 \pmod{\ell}$ that $\mathcal{F}(G) = \frac{\ell-2}{\ell^2-1} + \frac{1}{\ell^3-1} = \frac{\ell^3-\ell^2-1}{\ell^4+\ell^3-\ell-1}$, as desired. □

3.4 Images of the Arboreal Representation for Type II Reducible Elliptic Curves

We now consider the case where

$$\mathrm{im}\rho = \{M \in \mathrm{GL}_2(\mathbb{Z}_\ell) : M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}.$$

Our results in the previous two sections together with the fact that $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in \mathrm{im}\rho$ will make the Type II case much easier than the Type I case. We prove the following:

Theorem 3.10. *Let $\ell > 3$ be a fixed prime. Let E/F be a reducible elliptic curve of Type II. Suppose $G_{T_n/F} = \{M \in GL_2(\mathbb{Z}/\ell^n) : M \equiv \left(\begin{smallmatrix} * & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}$ and $\alpha \notin E(F) \cap \ell E(T_n)$. Then $im\omega_n$ is one of the following.*

1. $E[\ell^n] \rtimes G_{T_n/F}$
2. $\left\{(v, M) \in E[\ell^n] \rtimes G_{T_n/F} : v \equiv \left(\begin{smallmatrix} * \\ \gamma(d_0(M)-1) \end{smallmatrix}\right) \pmod{\ell}\right\}$ *for some fixed $\gamma \in \mathbb{Z}/\ell$.*

Proof. As in section 3.2, we use Propositions 3.2 and 3.3 to conclude that if $\alpha \notin E(F) \cap \ell E(T_n)$, then the image of κ_n is either $E[\ell^n]$ or $\left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$.

We are left to find all possible I-pairs (L, R, θ) for $L = (\mathbb{Z}/\ell^n)^2$ or $\left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$ and $R = G_{T_n/F}$. If $L = (\mathbb{Z}/\ell^n)^2$, then we are in case 1, so let $L = \left\langle \left(\begin{smallmatrix} 1 \\ 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} 0 \\ \ell \end{smallmatrix}\right) \right\rangle$. By Theorem 2.10, we must determine all maps $\theta : G_{T_n/F} \to (\mathbb{Z}/\ell^n)^2$ satisfying $\theta(MN) = \theta(M) - M.\theta(N)$ for all $M, N \in G_{T_n/F}$. Note that if we let M be any matrix $A \in G_{T_n/F}$ and set $N = -I$, then we have $\theta(-A) = \theta(A) + A.\theta(-I)$. On the other hand, if we set $M = -I$ and let N be any matrix $A \in G_{T_n/F}$, then $\theta(-A) = \theta(-I) - I.\theta(A) = \theta(-I) - \theta(A)$. We have then that for all $A \in G_{T_n/F}$, $2\theta(A) = -(A - I).\theta(-I)$. Thus, $\theta(A) = (A - I)v$ satisfies our condition for all $v \in (\mathbb{Z}/\ell^n)^2$. Fix $v = \left(\begin{smallmatrix} \epsilon \\ \gamma \end{smallmatrix}\right)$. By Theorem 2.10, we therefore obtain the following possible images of the arboreal

representation as subgroups of $\mathbb{Z}_\ell^2 \rtimes G_{T_\infty/F}$:

$$\begin{aligned}
&\{(u+\theta(M), M) : u \in \mathbb{Z}_\ell^2, M \in G_{T_\infty/F}\} \\
=&\{(u+(M-I)v, M) : u \in \mathbb{Z}_\ell^2, M \in G_{T_\infty/F}, v \in \mathbb{Z}_\ell^2\} \\
=&\{(u+\left(\begin{smallmatrix} a-1 & b \\ c & d-1 \end{smallmatrix}\right)\left(\begin{smallmatrix} \epsilon \\ \gamma \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) : u \in \mathbb{Z}_\ell^2, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_{T_\infty/F}\} \\
=&\{(u+\left(\begin{smallmatrix} (a-1)\epsilon+b\gamma \\ c\epsilon+(d-1)\gamma \end{smallmatrix}\right), \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)) : u \in \mathbb{Z}_\ell^2, \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in G_{T_\infty/F}\} \\
=&\{(u, M) : u \equiv \left(\begin{smallmatrix} * \\ \gamma(d_0(M)-1) \end{smallmatrix}\right) \pmod{\ell}, M \in G_{T_\infty/F}\}
\end{aligned}$$

since $c \equiv 0 \pmod{\ell}$. □

The condition $\alpha \notin E(F) \cap \ell E(T_n)$ for all $n \geq 1$ can be checked by simply checking the condition that $\alpha \notin \ell E(F)$ by the following proposition.

Proposition 3.11. *Let E be a Type II reducible elliptic curve. Then $E(F) \cap \ell E(T_n) = \ell E(F)$ for all $n \geq 1$.*

Proof. By Lemma 2.6, for a fixed $n \geq 1$, if $\mathrm{Hom}_{G_{T_1/F}}(N^{(n)}/N^{(n+1)}, E[\ell]) = 0$, then $E(F) \cap \ell E(T_n) = E(F) \cap \ell E(T_{n+1})$, where $N^{(n)} = G_{T_\infty/T_n}$ and $G_{T_1/F}$ acts on $N^{(n)}/N^{(n+1)}$ by conjugation. But since $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right) \in G_{T_1/F}$ acts trivially on $N^{(n)}/N^{(n+1)}$ for all $n \geq 1$ and acts by multiplication by -1 on $E[\ell]$, we conclude $\mathrm{Hom}_{G_{T_1/F}}(N^{(n)}/N^{(n+1)}, E[\ell]) = 0$ for all $n \geq 1$. Hence $E(F) \cap \ell E(T_n) = E(F) \cap \ell E(T_1)$ for all $n \geq 1$.

Now, Proposition 2.7 says that if there is a normal subgroup H of $G_{T_1/F}$ with order coprime to ℓ and $E[\ell]^H = 0$, then $E(F) \cap \ell E(T_1) = \ell E(F)$. Let $H = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \in G_{T_1/F}\}$. Then certainly H is normal with order coprime to ℓ. Further, since every element of H acts by multiplication by a, we have $E[\ell]^H = 0$. We conclude $E(F) \cap \ell E(T_n) = E(F) \cap \ell E(T_1) = \ell E(F)$ for all $n \geq 1$. □

3.5 The Density Computation for Type II Reducible Elliptic Curves

We are now ready to compute $\mathcal{F}(G)$ for Type II reducible elliptic curves for both cases (i) and (ii) in Theorem 3.10. We begin with case (i).

Theorem 3.12. *Suppose we are in case (i) in Theorem 3.10. Then*

$$\mathcal{F}(G) = \frac{\ell^5 - 2\ell^4 + 2\ell + 1}{\ell^5 - \ell^3 - \ell^2 + 1}.$$

Proof. Since the Kummer map is surjective, we may use Theorem 2.8. We must therefore compute

$$\begin{aligned}\mathcal{F}(G) &= \int_{M \in G_{T_n/F}} \ell^{-\mathrm{ord}_\ell(\det(M-I))} d\mu \\ &= \sum_{n=1}^{\infty} \frac{s_n}{\ell^{n-1} \# G_{T_n/F}}\end{aligned}$$

where $s_n = \{M \in G_{T_n/F} : \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n}\}$.

We begin by computing s_n for all $n \geq 1$. Let

$$r_n = \left\{ M \in G_{T_n/F} : \begin{array}{l} \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n}, \\ a_0(M) \equiv 1 \pmod{\ell} \end{array} \right\}.$$

and

$$r_n' = \left\{ M \in G_{T_n/F} : \begin{array}{l} \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n}, \\ a_0(M) \not\equiv 1 \pmod{\ell} \end{array} \right\}$$

Then $s_n = r_n + r_n'$. Note that r_n is precisely the quantity defined in Lemma 3.8, which we determined satisfies:

$$\sum_{n=1}^{\infty} \frac{r_n}{\ell^{5n-4}(\ell-1)} = \frac{\ell^3 - \ell - 1}{\ell^4 + \ell^3 - \ell - 1}.$$

Using the above together with $\# G_{T_n/F} = \ell^{4n-3}(\ell-1)^2$, we have then that

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{r_n}{\ell^{n-1} \# G_{T_n/F}} &= \sum_{n=1}^{\infty} \frac{r_n}{\ell^{5n-4}(\ell-1)^2} \\ &= \frac{1}{\ell-1}\left(\frac{\ell^3 - \ell - 1}{\ell^4 + \ell^3 - \ell - 1}\right) \\ &= \frac{\ell^3 - \ell - 1}{\ell^5 - \ell^3 - \ell^2 + 1}.\end{aligned}$$

We are left to compute r_n'. Let $M = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right)$, where $z \equiv 0 \pmod{\ell}$, $x \not\equiv 0, 1 \pmod{\ell}$, and $w \not\equiv 0 \pmod{\ell}$ (since M is invertible). Suppose $\det(M-I) \equiv t\ell^{n-1} \pmod{\ell^n}$ where $t \in (\mathbb{Z}/\ell)^\times$. First let $n = 1$. Then since $x - 1$ is a unit, we have that $w \equiv \frac{t}{x-1} + 1 \pmod{\ell}$ is completely determined. Note that for each value of x there is exactly one value of t (namely $t \equiv 1 - x$) that makes $w \equiv 0 \pmod{\ell}$, which cannot happen. So we have ℓ choices for y and $\ell - 2$ choices for each of x and t. We conclude that $r_1' = \ell(\ell-2)^2$. For $n \geq 2$ we still have $x - 1$ is a unit so that $w \equiv \frac{t\ell^{n-1} + yz}{x-1} + 1 \pmod{\ell^n}$, but there is no choice of t that makes w a nonunit. There are $\ell^{n-1}(\ell-2)$ choices for x, ℓ^n choices for y, ℓ^{n-1} choices for z, and $\ell - 1$ choices for t. We conclude that $r_n' = \ell^{3n-2}(\ell-1)(\ell-2)$ for $n \geq 2$.

We can now compute $\mathcal{F}(G)$. We have:

$$\begin{aligned}
\mathcal{F}(G) &= \sum_{n=1}^{\infty} \frac{s_n}{\ell^{n-1}\#G_{T_n/F}} \\
&= \sum_{n=1}^{\infty} \frac{r_n}{\ell^{n-1}\#G_{T_n/F}} + \sum_{n=1}^{\infty} \frac{r'_n}{\ell^{n-1}\#G_{T_n/F}} \\
&= \frac{\ell^3-\ell-1}{\ell^5-\ell^3-\ell^2+1} + \frac{\ell(\ell-2)^2}{\ell(\ell-1)^2} + \sum_{n=2}^{\infty} \frac{\ell^{3n-2}(\ell-1)(\ell-2)}{\ell^{5n-4}(\ell-1)^2} \\
&= \frac{\ell^3-\ell-1}{\ell^5-\ell^3-\ell^2+1} + \frac{(\ell-2)^2}{(\ell-1)^2} + \sum_{n=2}^{\infty} \frac{\ell-2}{\ell^{2n-2}(\ell-1)} \\
&= \frac{\ell^3-\ell-1}{\ell^5-\ell^3-\ell^2+1} + \frac{(\ell-2)^2}{(\ell-1)^2} + \frac{\ell-2}{(\ell-1)(\ell^2-1)} \\
&= \frac{\ell^5-2\ell^4+2\ell+1}{\ell^5-\ell^3-\ell^2+1}
\end{aligned}$$

□

We now compute $\mathcal{F}(G)$ in case (ii); that is, in the case

$$\mathrm{im}\omega_n \cong \left\langle \binom{1}{0}, \binom{0}{\ell} \right\rangle \rtimes G_{T_n/F}.$$

Theorem 3.13. *Suppose we are in case (ii) in Theorem 3.10. Then*

$$\mathcal{F}(G) = \frac{\ell^5-\ell^4-\ell^3-\ell^2+2\ell+2}{\ell^5-\ell^3-\ell^2+1}.$$

Proof. Note that since the Kummer map is not surjective, we cannot use Theorem 2.8. Recall from Proposition 2.4 that we have

$$\mathcal{F}(G) = \lim_{n\to\infty} \frac{\#\{(v,M) \in \mathrm{im}\omega_n : v \in \mathrm{im}(M-I)\}}{\#\mathrm{im}\omega_n}.$$

Fix $M \in G_{T_n/F}$ and $\gamma \in \mathbb{Z}/\ell$. We put the following group structure on $(\mathbb{Z}/\ell^n)^2$: for $u, v \in (\mathbb{Z}/\ell^n)^2$, we define $u \oplus v = u + v - \binom{\gamma b(M)}{\gamma(d(M)-1)}$. We now determine the size of the subgroup

$$H_M := \{v \equiv \binom{*}{\gamma(d_0(M)-1)} \pmod{\ell} : v \in \mathrm{im}(M-I)\}.$$

Let

$$H'_M = \{v \in (\mathbb{Z}/\ell^n)^2 : v \equiv \binom{*}{\gamma(d_0(M)-1)} \pmod{\ell}\}$$

and

$$H''_M = \{v \in (\mathbb{Z}/\ell^n)^2 : v \in \mathrm{im}(M-I)\}.$$

Then certainly $H_M = H'_M \cap H''_M$, so

$$|H_M| = \frac{|H'_M||H''_M|}{|H'_M H''_M|} = \frac{\ell^{2n-1} \cdot \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}}{|H'_M H''_M|}.$$

Now, if $d_0(M) \not\equiv 1 \pmod{\ell}$, then $v = \gamma' \binom{b(M)}{d(M)-1}$ for $\gamma' \neq \gamma$ is an element of H''_M that is not an element of H'_M. Since H'_M is index ℓ in $(\mathbb{Z}/\ell^n)^2$ and $H'_M H''_M$ is a subgroup of $(\mathbb{Z}/\ell^n)^2$ strictly larger than H'_M, we conclude $H'_M H''_M = (\mathbb{Z}/\ell^n)^2$, so that $|H_M| = \ell^{2n-\mathrm{ord}_\ell(\det(M-I))-1}$.

If $d_0(M) \equiv 1 \pmod{\ell}$, then $d_0(M)-1 \equiv 0 \pmod{\ell}$. Since $c(M) \equiv 0 \pmod{\ell}$, it follows that any $v \in \mathrm{im}(M-I)$ must satisfy $v \equiv \binom{*}{0} \pmod{\ell}$. Thus $H''_M \subseteq H'_M$, so that $|H'_M H''_M| = |H'_M| = \ell^{2n-1}$. We conclude $|H_M| = \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}$.

We have then that

$$\begin{aligned}
\mathcal{F}(G) &= \lim_{n\to\infty} \frac{\#\{(v,M) \in \mathrm{im}\omega_n : v \in \mathrm{im}(M-I)\}}{\#\mathrm{im}\omega_n} \\
&= \lim_{n\to\infty} \frac{\displaystyle\sum_{\substack{M \in G_{T_n/\mathbb{Q}} \\ d_0(M) \not\equiv 1}} \ell^{2n-\mathrm{ord}_\ell(\det(M-I))-1}}{\#G_{T_n/\mathbb{Q}}\ell^{2n-1}} \\
&\quad + \lim_{n\to\infty} \frac{\displaystyle\sum_{\substack{M \in G_{T_n/\mathbb{Q}} \\ d_0(M) \equiv 1}} \ell^{2n-\mathrm{ord}_\ell(\det(M-I))}}{\#G_{T_n/\mathbb{Q}}\ell^{2n-1}} \\
&= \sum_{n=1}^{\infty} \frac{s'_n}{\#G_{T_n/\mathbb{Q}}\ell^{n-1}} + \sum_{n=1}^{\infty} \frac{s''_n}{\#G_{T_n/\mathbb{Q}}\ell^{n-2}}.
\end{aligned}$$

where

$$s'_n = \#\left\{ M \in G_{T_n/\mathbb{Q}} : \begin{array}{l} d_0(M) \not\equiv 1 \pmod{\ell}, \\ \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n} \end{array} \right\}$$

and

$$s''_n = \#\left\{ M \in G_{T_n/\mathbb{Q}} : \begin{array}{l} d_0(M) \equiv 1 \pmod{\ell}, \\ \det(M-I) \equiv 0 \pmod{\ell^{n-1}}, \text{ but } \det(M-I) \not\equiv 0 \pmod{\ell^n} \end{array} \right\}.$$

We first compute s'_n. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where $a \not\equiv 0$, $c \equiv 0$, and $d \not\equiv 0, 1 \pmod{\ell}$ and let $\det(M-I) \equiv t\ell^{n-1} \pmod{\ell^n}$. Since $d-1$ is a unit, we have that $a \equiv \frac{t\ell^{n-1}+bc}{d-1} + 1 \pmod{\ell^n}$ is completely determined. In the case $n = 1$, for each choice of d there is one choice of t (namely $t = 1-d$) that makes $a \equiv 0 \pmod{\ell}$, which cannot happen. We have then that there are ℓ choices for b and $\ell - 2$ choices for each of d and t, giving us $s'_1 = \ell(\ell-2)^2$. For $n \geq 2$, no choice of t makes a a nonunit, so there are ℓ^m choices for b, ℓ^{m-1} choices for c, $\ell^{m-1}(\ell-2)$ choices for d and

$\ell - 1$ choices for t. We conclude $s'_n = \ell^{3n-2}(\ell-1)(\ell-2)$ for $n \geq 2$. We may now evaluate the first sum to be

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{s'_n}{\#G_{T_n/\mathbb{Q}}\ell^{n-1}} &= \frac{\ell(\ell-2)^2}{\ell(\ell-1)^2} + \sum_{n=2}^{\infty} \frac{\ell^{3n-2}(\ell-1)(\ell-2)}{\ell^{5n-4}(\ell-1)^2} \\ &= \frac{(\ell-2)^2}{(\ell-1)^2} + \frac{\ell-2}{\ell-1}\sum_{n=2}^{\infty}\frac{1}{\ell^{2n-2}} \\ &= \frac{(\ell-2)^2}{(\ell-1)^2} + \frac{\ell-2}{\ell-1}\left(\frac{1}{\ell^2-1}\right) \\ &= \frac{\ell^3-3\ell^2+\ell+2}{\ell^3-\ell^2-\ell+1}\end{aligned}$$

We now compute s''_n. Let

$$q''_n = \#\left\{ M \in G_{T_n/\mathbb{Q}} : \begin{array}{l} \det(M-I) \equiv t\ell^{n-1} (\text{mod } \ell^n), t \in (\mathbb{Z}/\ell)^\times, \\ d_0(M) \equiv 1 \text{ (mod } \ell), a_0(M) \not\equiv 1 (\text{mod } \ell) \end{array} \right\}$$

and

$$r''_n = \#\left\{ M \in G_{T_n/\mathbb{Q}} : \begin{array}{l} \det(M-I) \equiv t\ell^{n-1} (\text{mod } \ell^n), t \in (\mathbb{Z}/\ell)^\times, \\ d_0(M) \equiv 1 \text{ (mod } \ell), a_0(M) \equiv 1 (\text{mod } \ell) \end{array} \right\}.$$

Then certainly $s''_n = q''_n + r''_n$. Note that r''_n is precisely the quantity r_n defined in Lemma 3.8, which we know satisfies:

$$\sum_{n=1}^{\infty} \frac{r_n}{\ell^{5n-5}(\ell-1)} = \frac{\ell-1}{\ell^2-1} + \frac{1}{\ell^3-1} = \frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}.$$

We conclude that

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{r''_n}{\ell^{n-2}\#G_{T_n/F}} &= \frac{1}{\ell-1}\sum_{n=1}^{\infty}\frac{r''_n}{\ell^{5n-5}(\ell-1)} \\ &= \frac{\ell^3+\ell}{\ell^5-\ell^3-\ell^2+1}.\end{aligned}$$

We are left to find q''_n. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$, where $a \not\equiv 0, 1$, $c \equiv 0$, and $d \equiv 1 \text{ (mod } \ell)$. Let $\det(M - I) \equiv t\ell^{n-1} \text{ (mod } \ell^n)$ for $t \in (\mathbb{Z}/\ell)^\times$. Then since $a-1$ is a unit, we have $d \equiv \frac{t\ell^{n-1}+bc}{a-1} + 1 \text{ (mod } \ell^n)$ is completely determined. For $n = 1$, this determined d will never be congruent to 1 (mod ℓ), so $q''_1 = 0$. For $n \geq 2$, this determined d will always be congruent to 1 (mod ℓ). We therefore have $\ell^{n-1}(\ell-2)$ choices for a, ℓ^n choices for b, ℓ^{n-1} choices for c, and $\ell-1$ choices for t, giving us that

$q''_n = \ell^{3n-2}(\ell-1)(\ell-2)$ for $n \geq 2$. We thus compute the second sum to be

$$\begin{aligned}
\sum_{n=1}^{\infty} \frac{s''_n}{\#G_{T_n/F}\ell^{n-2}} &= \sum_{n=1}^{\infty} \frac{q''_n}{\#G_{T_n/F}\ell^{n-2}} + \sum_{n=1}^{\infty} \frac{r''_n}{\#G_{T_n/\mathbb{Q}}\ell^{n-2}} \\
&= \sum_{n=2}^{\infty} \frac{\ell^{3n-2}(\ell-1)(\ell-2)}{\ell^{5n-5}(\ell-1)^2} + \frac{\ell^3+\ell}{\ell^5-\ell^3-\ell^2+1} \\
&= \frac{\ell-2}{\ell-1} \sum_{n=2}^{\infty} \frac{1}{\ell^{2n-3}} + \frac{\ell^3+\ell}{\ell^5-\ell^3-\ell^2+1} \\
&= \frac{\ell-2}{\ell-1} \left(\frac{\ell}{\ell^2-1} \right) + \frac{\ell^3+\ell}{\ell^5-\ell^3-\ell^2+1} \\
&= \frac{\ell^4-\ell^2-\ell}{\ell^5-\ell^3-\ell^2+1}
\end{aligned}$$

We finally conclude that

$$\begin{aligned}
\mathcal{F}(G) &= \sum_{n=1}^{\infty} \frac{s'_n}{\#G_{T_n/F}\ell^{n-1}} + \sum_{n=1}^{\infty} \frac{s''_n}{\#G_{T_n/F}\ell^{n-2}} \\
&= \frac{\ell^3-3\ell^2+\ell+2}{\ell^3-\ell^2-\ell+1} + \frac{\ell^4-\ell^2-\ell}{\ell^5-\ell^3-\ell^2+1} \\
&= \frac{\ell^5-\ell^4-\ell^3-\ell^2+2\ell+2}{\ell^5-\ell^3-\ell^2+1}
\end{aligned}$$

as claimed.

□

CHAPTER 4

PRODUCTS OF ELLIPTIC CURVES

4.1 Preliminaries

In this chapter, we take A to be a product of elliptic curves with complex multiplication. If E is an elliptic curve over a number field F with complex multiplication, then $\mathrm{End}_{\bar{\mathbb{Q}}}(E) \cong R$, where R is an order in the complex multiplication quadratic field L. For a fixed prime ℓ we have the torsion representation ρ as defined in Chapter 2. Let $R_\ell := R \otimes \mathbb{Z}_\ell$. If $L \subseteq F$ and ℓ does not ramify in L or divide the index of R in the maximal order of L, then it is known $G_{T_\infty/\mathbb{Q}}$ — and thus the image of ρ — is isomorphic to a subgroup of $R_\ell^\times$ [22]. In addition, an analogue of Serre's open image theorem says that for any ℓ the image of ρ must have finite index in $R_\ell^\times$ and is exactly $R_\ell^\times$ for all but finitely many ℓ [19, Resume des cours de 1984-1985]. In this latter case, such a group is called a *Cartan subgroup*. For $L \not\subseteq F$, the image of ρ will be a subgroup of the normalizer N of some Cartan subgroup C, which contains C as a subgroup of index two. We consider the two cases where the image of ρ is either all of C or all of N.

In [10], necessary and sufficient conditions are determined for when the image of the arboreal representation is as large as possible for E an elliptic curve with complex multiplication. We reproduce the results below.

Proposition 4.1 ([10, Proposition 5.7])**.** *Let A be an elliptic curve defined over a number field F, and suppose that the image of $\rho : G_{T_\infty/F} \to GL_2(\mathbb{Z}_\ell)$ is contained in the normalizer N of a Cartan subgroup but not in a Cartan subgroup. Denote by N_m the image of N in $GL(\mathbb{Z}/\ell^m\mathbb{Z})$. If $\ell \geq 3$, then ρ maps onto N if and only if $G_{T_2/F} \cong N_2$. For $\ell = 2$, the same conclusion holds if and only if $G_{T_3/F} \cong N_3$.*

Proposition 4.2 ([10, Theorem 5.8])**.** *Let A be an elliptic curve defined over a number field F, and suppose that the image of $\rho : G_{T_\infty/F} \to GL_2(\mathbb{Z}_\ell)$ is the full normalizer N of a Cartan*

subgroup. Suppose further that we are not in the case where $\ell = 2$ and the underlying Cartan subgroup is split. Then the Kummer map $\kappa : G_{K_\infty/T_\infty} \to \mathbb{Z}_\ell^2$ is surjective if and only if $\alpha \notin \ell A(F)$. Replacing N with C and N_m with C_m gives an analogous statement for when ρ surjects onto a nonsplit Cartan subgroup C.

Corollary 4.3 ([10, Corollary 5.9])**.** *Let N be as in Proposition 4.2 and let $\ell \geq 3$. The arboreal representation $\omega : G_{K_\infty/K} \to \mathbb{Z}_\ell^2 \rtimes N$ is surjective if and only if the conditions of Propositions 4.1 and 4.2 are satisfied.*

Let $A = E_1 \times \cdots \times E_m$ be the product of elliptic curves E_i/F_i with complex multiplication. Fix a prime $\ell \geq 3$. For each i, choose $\alpha_i \in E_i(F_i)$ and assume the conditions of Propositions 4.1 and 4.2 are satisfied, so that the Kummer map is surjective. Then the image of each ω_i is the full group $\mathbb{Z}_\ell^2 \rtimes C_i$ (resp. $\mathbb{Z}_\ell^2 \rtimes N_i$), where C_i is a Cartan subgroup (resp. N_i is the normalizer of a Cartan subgroup). Since the ℓ^n torsion fields for each E_i contain the ℓ^n roots of unity, the image of the torsion representation ρ attached to A can be no larger than $\{(M_1, \ldots, M_m) \in C_1 \times \ldots \times C_m : \det(M_1) = \cdots = \det(M_m)\}$. We thus introduce the definition of appropriately intersecting torsion fields, which is a sufficient condition for when the image of ρ will be this largest possible set.

Definition 4.4. *For $i = 1, 2, \ldots, m$, let E_i/F_i be an elliptic curve with complex multiplication. Let $T_\infty^i = F_i(E_i[\ell^\infty])$, $F = F_1F_2 \cdots F_m$, and $F^i = F_1 \cdots F_{i-1}F_{i+1} \cdots F_m$. We say the E_i have* appropriately intersecting torsion fields *if $T_\infty^i F^i \cap T_\infty^j F^j = F(\zeta_{\ell^\infty})$ for all $i \neq j$, $F_i \cap F = F_i$ for all i, and $T_\infty^i \cap F(\zeta_{\ell_\infty}) = F_i(\zeta_{\ell_\infty})$ for all i.*

4.2 Images of the Arboreal Representation for the Split Case

We now determine the image of the torsion representation under the assumption that the E_i have appropriately intersecting torsion fields. We begin with the split case.

Proposition 4.5. *For $i = 1, 2, \ldots, m$, let E_i be an elliptic curve with complex multiplication defined over its complex quadratic multiplication field F_i. Fix a prime $\ell \geq 3$ and suppose we are in the split case for each E_i and the image of each ρ_i is a full Cartan subgroup C_i. Furthermore, assume the E_i have appropriately intersecting torsion fields and let $T_\infty = T_\infty^1 T_\infty^2 \cdots T_\infty^m$. Then $G := Gal(T_\infty/F) \cong (\mathbb{Z}_\ell^\times)^{m+1}$.*

Proof. For $i = 1, 2, \ldots, m$, let $T_n^i = F_i(E_i[\ell^n])$ and set $T_n = T_n^1 T_n^2 \cdots T_n^m$. By hypothesis, since the E_i have appropriately intersecting torsion fields, we have

$$G_i := \mathrm{Gal}(T_n^i F^i / F) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times \times (\mathbb{Z}/\ell^n\mathbb{Z})^\times.$$

We first show $\mathrm{Gal}(T_n^i F^i / F(\zeta_{\ell^n})) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$.

Lemma 4.6. *Let C be a finite cyclic group and fix $r > 0$. Furthermore, let G be a subgroup of C^r with normal subgroup H such that $G/H \cong C$. Then $G \cong C^n$ if and only if $H \cong C^{n-1}$.*

Proof. Let $\bar{x}$ be the image of an element $x \in G$ in G/H such that $\bar{x}$ generates G/H. Let K be the subgroup of G generated by x. Since every element of G has order divisible by $|C|$, we have $x^{|C|} = 1$. Furthermore, since $\bar{x}$ generates $G/H \cong C$, we have $\bar{x}$ has order exactly $|C|$. It follows that x has order exactly $|C|$ and thus that $K \cong C$. Now, if there were an $m < |C|$ such that $x^m \in H$, then $\bar{x}^m \in H$, contradicting that $\bar{x}$ generates G/H. We therefore have $H \cap K = \{1\}$. It follows that $G \cong H \times K$. Thus, if $G \cong C^n$, then by the structure theorem, we have $H \cong C^{n-1}$ and if $H \cong C^{n-1}$, then $G \cong C^{n-1} \times C \cong C^n$. □

Since $\mathrm{Gal}(F(\zeta_{\ell^n})/F) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$, applying Lemma 4.6 with $G = G_i$ gives us that $H_i := \mathrm{Gal}(T_n^i F^i / F(\zeta_{\ell^n})) \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$.

We know from Galois theory that $H := G_{T_n/F(\zeta_{\ell^n})} = H_1 \times H_2 \times \ldots \times H_m \cong [(\mathbb{Z}/\ell^n\mathbb{Z})^\times]^m$ and that $G/H = G_{F(\zeta_{\ell^n})/F} \cong (\mathbb{Z}/\ell^n\mathbb{Z})^\times$. Applying Lemma 4.6 again gives us that $H \cong [(\mathbb{Z}/\ell^n\mathbb{Z})^\times]^{m+1}$.

Taking the inverse limit gives our desired result.

□

Corollary 4.7. *For each elliptic curve E_i with complex multiplication defined over its complex multiplication field F_i, suppose the E_i have appropriately intersecting torsion fields, $\mathrm{im}\rho_i \cong C_i$, and that each C_i is a split Cartan subgroup. Then $\mathrm{im}\rho \cong H := \{(M_1, \ldots, M_m) \in C_1 \times \ldots \times C_m : \det(M_1) = \cdots = \det(M_m)\}$.*

Proof. Our result follows from the intersection condition $T_\infty^i F^i \cap T_\infty^j F^j = F(\zeta_{\ell^\infty})$ for all $i \neq j$ and the fact that $G_{F(\zeta_{\ell^\infty})/F}$ is given by the cyclotomic character. □

Corollary 4.8. *For $i = 1, 2, \ldots, m$, let E_i be an elliptic curve with complex multiplication defined over its complex quadratic multiplication field F_i satisfying the conditions of Proposition 4.5.*

Assume the Kummer map is surjective. Then the arboreal representation $\omega : G_{K_\infty/F} \to \mathbb{Z}_\ell^{2m} \rtimes H$ *is surjective.*

4.3 The Density Computation for the Split Case

Theorem 4.9. *Let* $A = E_1 \times E_2 \times \ldots \times E_m$*, where for each* $i = 1, 2, \ldots, m$*,* E_i *is an elliptic curve with complex multiplication defined over its complex quadratic multiplication field* F_i*. Fix a prime* $\ell \geq 3$*. Suppose we are in the split case for each* E_i *and the image of each* ρ_i *is a full Cartan subgroup* C_i*. Further, assume the* E_i *have appropriately intersecting torsion fields and the Kummer map is surjective. Then* $\mathcal{F}(G) = \frac{(\ell-2)(\ell^2-2\ell-1)^m}{(\ell-1)^{m+1}(\ell+1)^m} + \left(\frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i (-1)^{m-i}}{\ell^{3m-3i+1}-1}$.

Proof. We begin with the following lemma.

Lemma 4.10. *Let* C *be any of the split Cartan subgroups,* C_i *and let* $\bar{C}$ *be its reduction* $(mod\ \ell^n)$ *for fixed* $n \geq 1$*. Define*

$$s_{D,k} = \#\{M \in \bar{C} : detM \equiv D \ (mod\ \ell^n) \text{ and } ord_\ell(det(M-I)) = k\}.$$

For $D \not\equiv 1\ (mod\ \ell)$*,*

$$s_{D,k} = \begin{cases} (\ell-3)\ell^{n-1}, & \text{if } k = 0 \\ 2(\ell-1)\ell^{n-k-1}, & \text{if } 1 \leq k \leq n-1 \end{cases}$$

For $ord_\ell(D-1) = j > 0$*,*

$$s_{D,k} = \begin{cases} (\ell-2)\ell^{n-1}, & \text{if } k = 0 \\ 0, & \text{if } k = 1, 3, \ldots, 2j-1 \\ (\ell-1)\ell^{n-\frac{k}{2}-1}, & \text{if } k = 2, 4, \ldots, 2j-2 \\ (\ell-2)\ell^{n-\frac{k}{2}-1}, & \text{if } k = 2j \\ 2(\ell-1)\ell^{n+j-k-1}, & \text{if } 2j+1 \leq k \leq n-1 \end{cases}$$

Proof. Fix D and let $M = \left(\begin{smallmatrix} a & 0 \\ 0 & b \end{smallmatrix}\right)$ have determinant D. Then since $ab \equiv D \pmod{\ell^n}$, we have $\det(M-I) = (a-1)(b-1) = \frac{(a-1)(D-a)}{a}$. Thus, $s_{D_k} = \#S_{D,k}$, where

$$S_{D,k} = \{a \in (\mathbb{Z}/\ell^n)^\times : \mathrm{ord}_\ell(a-1) + \mathrm{ord}_\ell(D-a) = k\}.$$

If $D \not\equiv 0 \pmod{\ell}$, then for all a, at least one of $\mathrm{ord}_\ell(a-1)$ or $\mathrm{ord}_\ell(D-a)$ is zero. We see then that $a \in S_{D,0}$ if and only if $a \not\equiv 1 \pmod{\ell}$ and $a \not\equiv D \pmod{\ell}$. Hence, $s_{D,0} = (\ell-3)\ell^{n-1}$. Similarly, for $1 \leq k \leq n-1$, $a \in S_{D,k}$ if and only if $a \equiv 1 \pmod{\ell^k}$, but not $\pmod{\ell^{k+1}}$ or $a \equiv D \pmod{\ell^k}$, but not $\pmod{\ell^{k+1}}$. We therefore have $s_{D,k} = 2(\ell-1)\ell^{n-k-1}$ for $1 \leq k \leq n-1$, as claimed.

Suppose $\mathrm{ord}_\ell(D-1) = j > 0$. Then $a \in S_{D,0}$ if and only if $a \not\equiv 1 \pmod{\ell}$. Thus, $s_{D,0} = (\ell-3)\ell^{n-1}$. Since $D \equiv 1 \pmod{\ell^j}$, we have $a - 1 \equiv a - D \pmod{\ell^j}$. Hence, if $k < 2j$ is odd, then $s_{D,k} = 0$. If $k < 2j$ is even and $a \in S_{D,k}$, then $\mathrm{ord}_\ell(a-1) = \mathrm{ord}_\ell(D-a) = \frac{k}{2}$, so that $s_{D,k} = (\ell-1)\ell^{n-\frac{k}{2}-1}$. If $k = 2j$, then $a \in S_{D,k}$ if and only if $\mathrm{ord}_\ell(a-1) = \mathrm{ord}_\ell(D-a) = j$. Since $a - 1 \not\equiv a - D \pmod{\ell^{j+1}}$, we have $s_{D,k} = (\ell-2)\ell^{n-\frac{k}{2}-1}$. Finally, if $2j+1 \leq k \leq n-1$, then $a \in S_{D,k}$ if and only if $\mathrm{ord}_\ell(a-1) = j$ and $\mathrm{ord}_\ell(D-a) = k-j$ or $\mathrm{ord}_\ell(a-1) = k-j$ and $\mathrm{ord}_\ell(D-a) = j$. Thus, $s_{D,k} = 2(\ell-1)\ell^{n+j-k-1}$. □

To compute $\mathcal{F}(G)$, consider the function $f_D(x) = \sum_{k=0}^{n-1} s_{D,k} x^k$ for fixed D and n. We know from Proposition 2.8 that

$$\begin{aligned}
\mathcal{F}(G) &= \int_{M \in G_{T_\infty/F}} \prod_{i=1}^{m} \ell^{-\mathrm{ord}_\ell(\det(M_i - I))}\, dM \\
&= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{\#\{(M_1,\ldots,M_m) \in G_{T_n/F} : \sum_{i=1}^m \mathrm{ord}_\ell(\det(M_i - I)) = k\}}{\ell^k \# G_{T_n/F}} \\
&= \lim_{n\to\infty} \frac{\sum_{D \in (\mathbb{Z}/\ell^n)^\times} \left[f_D\left(\frac{1}{\ell}\right)\right]^m}{[(\ell-1)\ell^{n-1}]^{m+1}}.
\end{aligned}$$

Now, using Lemma 4.10 it can be shown that

$$f_D\left(\frac{1}{\ell}\right) = \begin{cases} (\ell-3)\ell^{n-1} + \frac{2(\ell^{2n-2}-1)}{(\ell+1)\ell^{n-1}}, & \text{if } \mathrm{ord}_\ell(D-1) = 0 \\ \ell^n - 2\ell^{n-1} + \frac{(\ell^{3j-3}-1)\ell^{n-3j+2}}{\ell^2+\ell+1} + \ell^{n-3j} & \text{if } \mathrm{ord}_\ell(D-1) = j > 0. \\ \quad - 2\ell^{n-3j-1} + \frac{2(\ell^{2n-4j-2}-1)\ell^{j+1-n}}{\ell+1}, & \end{cases}$$

We therefore obtain

$$\begin{aligned}\mathcal{F}(G) &= \frac{(\ell-2)}{\ell-1}\left[\frac{\ell^2-2\ell-1}{\ell^2-1}\right]^m + \left(\frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}\right)^m \sum_{j=1}^{\infty} \frac{\left[\ell^{3j}\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}-1\right]^m}{\ell^{(3m+1)j}} \\ &= \frac{(\ell-2)(\ell^2-2\ell-1)^m}{(\ell-1)^{m+1}(\ell+1)^m} \\ &\quad + \left(\frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}\right)^m \sum_{i=0}^{m}\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i (-1)^{m-i}\sum_{j=1}^{\infty}\frac{1}{\ell^{(3m-3i+1)j}} \\ &= \frac{(\ell-2)(\ell^2-2\ell-1)^m}{(\ell-1)^{m+1}(\ell+1)^m} + \left(\frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}\right)^m \sum_{i=0}^{m}\frac{\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i(-1)^{m-i}}{\ell^{3m-3i+1}-1},\end{aligned}$$

as desired.

□

Corollary 4.11. *For $m = 1$,*

$$\mathcal{F}(G) = \left(\frac{\ell^2-\ell-1}{\ell^2-1}\right)^2.$$

For $m = 2$,

$$\mathcal{F}(G) = \frac{\ell^{11}-4\ell^{10}+4\ell^9+\ell^8-2\ell^6-2\ell^5-2\ell^4+\ell^3-4\ell^2-4\ell-1}{(\ell^2-1)^2(\ell^7-1)}.$$

For $m = 3$,

$$\begin{aligned}\mathcal{F}(G) = (&\ell^{22}-5\ell^{21}+7\ell^{20}+2\ell^{19}-6\ell^{18}-5\ell^{17}-5\ell^{16}+3\ell^{15}+9\ell^{14}+6\ell^{13}+14\ell^{12}+26\ell^{11} \\ &+26\ell^{10}+28\ell^9+37\ell^8+37\ell^7+35\ell^6+29\ell^5+22\ell^4+24\ell^3+19\ell^2+7\ell+1)/ \\ &[(\ell^2-1)^2(\ell^7-1)(\ell^{10}-1)(\ell+1)].\end{aligned}$$

Corollary 4.12. *Assume the hypotheses of the previous theorem. Then*

$$\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \frac{\ell^2-\ell-1}{\ell^2-\ell} \le \mathcal{F}(G) \le \left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \frac{\ell^2+2\ell-4}{\ell^2-\ell}.$$

In particular,

$$\mathcal{F}(G) = \left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \left(1+O\left(\frac{1}{\ell}\right)\right).$$

Proof. From the theorem above, we know

$$\mathcal{F}(G) = \frac{\ell-2}{\ell-1}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m + \left(\frac{\ell^3+\ell}{\ell^4+\ell^3-\ell-1}\right)^m \sum_{i=0}^{m}\frac{\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i(-1)^{m-i}}{\ell^{3m-3i+1}-1}.$$

Since $\ell^{3m-3i+1}-1 \le \ell^{3m-3i+1}$, we have

$$\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i (-1)^{m-i}}{\ell^{3m-3i+1}-1}$$
$$\geq \frac{1}{\ell}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \sum_{i=0}^{m} \binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i \left(\frac{-1}{\ell^3}\right)^{m-i}$$
$$= \frac{1}{\ell}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}-\frac{1}{\ell^3}\right)^m$$
$$= \frac{1}{\ell}\left(\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right)^m$$

Thus, $\mathcal{F}(G) \geq \frac{\ell-2}{\ell-1}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m + \frac{1}{\ell}\left(\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right)^m$. Noting that $\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)} \geq \frac{\ell^2-2\ell-1}{\ell^2-1}$, we conclude

$$\begin{aligned}\mathcal{F}(G) &\geq \frac{\ell-2}{\ell-1}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m + \frac{1}{\ell}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \\ &= \left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \frac{\ell^2-\ell-1}{\ell^2-\ell}.\end{aligned}$$

To see the upper bound, we use $\ell^{3m-3i+1}-1 \geq \frac{1}{2}\ell^{3m-3i+1}$, so that

$$\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i (-1)^{m-i}}{\ell^{3m-3i+1}-1}$$
$$\leq \frac{2}{\ell}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \sum_{i=0}^{m} \binom{m}{i}\left(\frac{\ell^4-2\ell^2-2\ell-1}{\ell^3+\ell}\right)^i \left(\frac{-1}{\ell^3}\right)^{m-i}$$
$$= \frac{2}{\ell}\left(\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right)^m.$$

Thus, $\mathcal{F}(G) \leq \frac{\ell-2}{\ell-1}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m + \frac{2}{\ell}\left(\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)}\right)^m$. Noting that $\frac{\ell^4-\ell^3-2\ell^2+\ell-1}{\ell^2(\ell^2-1)} \leq 2\frac{\ell^2-2\ell-1}{\ell^2-1}$, we conclude

$$\begin{aligned}\mathcal{F}(G) &\leq \frac{\ell-2}{\ell-1}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m + \frac{4}{\ell}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \\ &= \left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^m \frac{\ell^2+2\ell-4}{\ell^2-\ell},\end{aligned}$$

as claimed. The second statement follows immediately.

□

We now consider the product of elliptic curves E_i/F_i such that the image of each torsion representation is the normalizer of a Cartan subgroup. As mentioned above, this will occur when each complex multiplication field L_i is not contained in F_i.

Theorem 4.13. *Let $A = E_1 \times E_2 \times \ldots \times E_m$, where for each $i = 1, 2, \ldots, m$, E_i/F_i is an elliptic curve with complex multiplication. Fix a prime $\ell \geq 3$. Suppose we are in the split case for each E_i and the image of each ρ_i is the full normalizer N_i of a Cartan subgroup C_i. Further, assume the E_i have appropriately intersecting torsion fields and the Kummer map is surjective. Then*

$$\mathcal{F}(G) = \frac{\ell-3}{\ell-1}\left[\frac{\ell^2-\ell-1}{\ell^2-1}\right]^m + \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\left(\frac{\ell^2-2\ell-1}{\ell^2-1}\right)^{m-j}\frac{1}{\ell^{j+1}-1} + \frac{1}{2^m(\ell^3-1)^m}\sum_{i=0}^{m}\binom{m}{i}(2\ell^3-\ell^2-\ell-2)^{m-i}\left(\frac{\ell^3+\ell}{\ell+1}\right)^i\frac{(-1)^i}{\ell^{3i+1}-1}$$

Proof. Let N be the normalizer of any of the split Cartan subgroups, C. Let $\bar{N}$ be the reduction of $N \pmod{\ell^n}$ for fixed $n \geq 1$. Define

$$\tilde{s}_{D,k} = \#\{M \in \bar{N} : \det M \equiv D \pmod{\ell^n} \text{ and } \mathrm{ord}_\ell(\det(M-I)) = k\}.$$

Note for $M \in N\backslash C$ that $\det(M-I) = 1 + \det M$. It follows that

$$\tilde{s}_{D,k} = \begin{cases} s_{D,k} + (\ell-1)\ell^{n-1}, & \text{if } k = \mathrm{ord}_\ell(D+1) \\ s_{D,k}, & \text{otherwise,} \end{cases}$$

where $s_{D,k}$ is the quantity defined in Lemma 4.10.

To compute $\mathcal{F}(G)$, consider the function $\tilde{f}_D(x) = \sum_{k=0}^{n}\tilde{s}_{D,k}x^k$ for fixed D and n. Using $\tilde{s}_{D,k}$ described above and $f_D(x)$ defined in the proof of Theorem 4.9, we conclude:

$$\tilde{f}_D\left(\frac{1}{\ell}\right) = f_D\left(\frac{1}{\ell}\right) + \frac{(\ell-1)\ell^{n-1}}{\ell^i},$$

where $i = \mathrm{ord}_\ell(D+1)$.

We know from Proposition 2.8 that

$$\begin{aligned}\mathcal{F}(G) &= \int_{M \in G_{T_\infty/F}} \prod_{i=1}^{m} \ell^{-\mathrm{ord}_\ell(\det(M_i - I))}\, dM \\ &= \lim_{n\to\infty}\sum_{k=0}^{n}\frac{\#\{(M_1,\ldots,M_m) \in G_{T_n/F} : \sum_{i=1}^m \mathrm{ord}_\ell(\det(M_i-I)) = k\}}{\ell^k \# G_{T_n/F}} \\ &= \lim_{n\to\infty}\frac{\sum_{D\in(\mathbb{Z}/\ell^n)^\times}\left[\tilde{f}_D\left(\frac{1}{\ell}\right)\right]^m}{2^m[(\ell-1)\ell^{n-1}]^{m+1}}.\end{aligned}$$

With some computation, it can be shown that the three sums given in the expression for $\mathcal{F}(G)$ in the statement of the theorem correspond to the cases $D \not\equiv -1, 1 \pmod{\ell}$, $D \equiv -1 \pmod{\ell}$, and $D \equiv 1 \pmod{\ell}$, respectively.

□

Corollary 4.14. *For $m = 1$,*

$$\mathcal{F}(G) = \frac{1}{2}\left(\frac{\ell^2-\ell-1}{\ell^2-1}\right)\left[1+\frac{\ell^2-\ell-1}{\ell^2-1}\right].$$

For $m = 2$,

$$\mathcal{F}(G) = \frac{4\ell^{13}-7\ell^{12}-4\ell^{11}+\ell^{10}+16\ell^9+9\ell^8-\ell^7-9\ell^6+\ell^5-7\ell^3-20\ell^2-15\ell-4}{4(\ell-1)^3(\ell+1)^2(\ell^2+\ell+1)(\ell^6+\ell^5+\ell^4+\ell^3+\ell^2+\ell+1)}.$$

4.4 The Nonsplit Case

We have similar results for the nonsplit case. We begin with a proposition similar to Proposition 4.5, whose proof we omit.

Proposition 4.15. *For $i = 1, 2, \ldots, m$, let E_i be an elliptic curve with complex multiplication defined over its complex quadratic multiplication field F_i. Fix a prime $\ell \geq 3$ and suppose we are in the nonsplit case for each E_i and the image of each ρ_i is a full Cartan subgroup C_i. Furthermore, assume the E_i have appropriately intersecting torsion fields and let $T_\infty = T_\infty^1 T_\infty^2 \cdots T_\infty^m$. Then $G := Gal(T_\infty/F) \cong \{(M_1, \ldots, M_m) \in C_1 \times \ldots \times C_m : det(M_1) = \cdots = det(M_m)\}$.*

We can now compute the density $\mathcal{F}(G)$.

Theorem 4.16. *Let $A = E_1 \times E_2 \times \ldots \times E_m$, where for each $i = 1, 2, \ldots, m$, E_i is an elliptic curve with complex multiplication defined over its complex quadratic multiplication field F_i. Fix a prime $\ell \geq 3$ and choose $\alpha_i \notin \ell E_i(F_i)$. Suppose we are in the nonsplit case for each E_i and the image of each ρ_i is a full Cartan subgroup C_i. Further, assume the E_i have appropriately intersecting torsion fields and the Kummer map is surjective. Then $\mathcal{F}(G) = \frac{\ell-2}{\ell-1} + \left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1}$.*

Proof. We begin with the following lemma.

Lemma 4.17. *Let C be any of the nonsplit Cartan subgroups C_i and $\bar{C}$ be its reduction $(mod\ \ell^n)$ for fixed $n \geq 1$. Note that for all M in $\bar{C}$, we have $ord_\ell(det(M-I))$ must be even. Let*

$$r_{D,k} = \#\{M \in \bar{C} : detM \equiv D\ (mod\ \ell^n)\ and\ ord_\ell(det(M-I)) = 2k\}.$$

For $k = 0$,

$$r_{D,0} = \begin{cases} (\ell+1)\ell^{n-1}, & \text{if } D \not\equiv 1 \ (mod\ \ell). \\ \ell^n, & \text{if } D \equiv 1 \ (mod\ \ell) \end{cases}$$

For $ord_\ell(D-1) = j$ and $1 \leq k \leq n$,

$$r_{D,k} = \begin{cases} 0, & \text{if } j = 0 \\ (\ell-1)\ell^{n-k-1}, & \text{if } k < j \\ \ell^{n-k}, & \text{if } k = j \neq 0 \\ 0, & \text{otherwise.} \end{cases}$$

Proof. We know $C \cong R_\ell^\times$, where R is an order in a complex quadratic field and $R_\ell = R \otimes \mathbb{Z}_\ell$. Fix $D \in (\mathbb{Z}/\ell^n)^\times$. Then $M \in \bar{C}$ with determinant D corresponds to $a \in R_\ell$ such that $D \equiv N(a) \pmod{\ell^n}$, where $N : R_\ell \longrightarrow^\times \mathbb{Z}_\ell^\times$ is the norm map. Thus, $r_{D,k} = \#R_{D,k}$, where

$$\begin{aligned} R_{D,k} &= \{a \in R_\ell^\times : N(a) \equiv D \pmod{\ell^n} \text{ and } \mathrm{ord}_\ell(N(a-1)) = 2k\} \\ &= \{a \in R_\ell^\times : N(a) \equiv D \pmod{\ell^n} \text{ and } \mathrm{ord}_\ell(a-1) = k\} \end{aligned}$$

Note that $\mathrm{ord}_\ell(a-1)$ is exactly k if and only if the ℓ-adic expansion of a has constant term 1, order i term 0 for $1 \leq i \leq k-1$, and order k term nonzero.

Let $k = 0$. If $D \not\equiv 1 \pmod{\ell}$, then $N(a) = D$ if and only if $\mathrm{ord}_\ell(a-1) = 0$. Let $\bar{N}$ be the norm map $(\mathrm{mod}\ \ell^n)$. Then $r_{D,0} = \#\{a \in R_\ell^\times : \bar{N}(a) \equiv D \pmod{\ell^n}\} = (\ell+1)\ell^{n-1}$, since $\bar{N}$ is surjective. If $D \equiv 1 \pmod{\ell}$, then of the $(\ell+1)\ell^{n-1}$ elements $R_\ell^\times$ with norm D, precisely ℓ^{n-1} have constant term 1. Thus, $r_{D,0} = (\ell+1)\ell^{n-1} - \ell^{n-1} = \ell^n$, as claimed.

Let $\mathrm{ord}_\ell(D-1) = j$ and $k \geq 1$. Since $k \geq 1$, if $a \in R_{D,k}$, then by the note above, a has constant term 1, so that $N(a) \equiv 1 \pmod{\ell}$. It follows that $r_{D,k} = 0$ if $j = 0$. Let $j > 0$. There are ℓ^{n-k} elements of $R_\ell^\times$ with norm D, constant term 1, and order i term 0 for $1 \leq i \leq k-1$. If $k = j$, all of these have order k term nonzero. If $k < j$, then exactly ℓ^{n-k-1} have k term zero. It follows that $r_{D,k} = \ell^{n-k} - \ell^{n-k-1} = (\ell-1)\ell^{n-k-1}$ for $k < j$ and $r_{D,k} = \ell^{n-k}$ for $k = j$. Finally, it is clear if $k > j$, then $r_{D,k} = 0$. □

To compute $\mathcal{F}(G)$, consider the function $g_D(x) = \sum_{k=0}^{n} r_{D,k} x^{2k}$ for fixed n and D. We have

from Proposition 2.8 that

$$\begin{aligned}\mathcal{F}(G) &= \int_{M\in G_{T_\infty/F}} \prod_{i=1}^{m} \ell^{-\mathrm{ord}_\ell(\det(M_i-I))}\, dM \\ &= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{\#\{(M_1,\dots,M_m)\in G_{T_n/F} : \sum_{i=1}^m \mathrm{ord}_\ell(\det(M_i-I))=k\}}{\ell^k \# G_{T_n/F}} \\ &= \lim_{n\to\infty} \frac{\sum_{D\in(\mathbb{Z}/\ell^n)^\times}\left[g_D\left(\frac{1}{\ell}\right)\right]^m}{(\ell-1)\ell^{n-1}[(\ell+1)\ell^{n-1}]^m}.\end{aligned}$$

Now, using Lemma 4.17, it can be shown that

$$g_D\left(\frac{1}{\ell}\right) = \begin{cases} (\ell+1)\ell^{n-1}, & \text{if } D\not\equiv 1 \pmod{\ell} \\ \frac{\ell^{n-1}}{\ell^2+\ell+1}\left(\ell^3+\ell^2+\ell+1+\frac{\ell+1}{\ell^{3j-1}}\right), & \text{if } \mathrm{ord}_\ell(D-1)=j>0. \end{cases}$$

We therefore obtain

$$\begin{aligned}\mathcal{F}(G) &= \lim_{n\to\infty}\Bigg[\frac{(\ell-2)\ell^{n-1}\left[(\ell+1)\ell^{n-1}\right]^m}{(\ell-1)\ell^{n-1}\left[(\ell+1)\ell^{n-1}\right]^m} \\ &\qquad + \sum_{j=1}^{n-1}\frac{(\ell-1)\ell^{n-j-1}\left[\frac{\ell^{n-1}}{\ell^2+\ell+1}\left(\ell^3+\ell^2+\ell+1+\frac{\ell+1}{\ell^{3j-1}}\right)\right]^m}{(\ell-1)\ell^{n-1}\left[(\ell+1)\ell^{n-1}\right]^m}\Bigg] \\ &= \frac{\ell-2}{\ell-1} + \left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m}\binom{m}{i}(\ell^2+1)^{m-i}\ell^i \sum_{j=1}^{\infty}\frac{1}{\ell^{(3i+1)j}} \\ &= \frac{\ell-2}{\ell-1} + \left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m}\frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1},\end{aligned}$$

as desired. □

Corollary 4.18. *For $m=1$,*

$$\mathcal{F}(G) = \frac{\ell^4-\ell^2-1}{\ell^4-1}.$$

For $m=2$,

$$\mathcal{F}(G) = \frac{\ell^8+\ell^7-2\ell^6-\ell^5-\ell^3-2\ell^2-\ell-1}{(\ell+1)(\ell^7-1)}.$$

For $m=3$,

$$\mathcal{F}(G) = \frac{\ell^{16}+\ell^{15}-2\ell^{14}+\ell^{13}-3\ell^{12}-\ell^{11}-5\ell^{10}-9\ell^8-7\ell^6-3\ell^5-5\ell^4-\ell^3-4\ell^2-\ell-1}{(\ell-1)(\ell+1)(\ell^4-\ell^3+\ell^2-\ell+1)(\ell^4+\ell^3+\ell^2+\ell+1)(\ell^6+\ell^5+\ell^4+\ell^3+\ell^2+\ell+1)}.$$

Corollary 4.19. *Assume the hypotheses of the previous theorem. Then*

$$\frac{\ell-2}{\ell-1} + \frac{1}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m \le \mathcal{F}(G) \le \frac{\ell-2}{\ell-1} + \frac{2}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m.$$

Proof. From the theorem above, we know

$$\mathcal{F}(G) = \frac{\ell-2}{\ell-1} + \left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1}.$$

Thus, it is enough to show

$$\frac{1}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m \leq \left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1} \leq \frac{2}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m.$$

Since $\ell^{3i+1}-1 \leq \ell^{3i+1}$, we have

$$\begin{aligned}\left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1} &\geq \frac{1}{\ell}\left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \binom{m}{i}(\ell^2+1)^{m-i}\left(\frac{1}{\ell^2}\right)^i \\ &= \frac{1}{\ell}\left(\frac{1}{\ell^2+\ell+1}\right)^m \left[\ell^2+1+\frac{1}{\ell^2}\right]^m \\ &= \frac{1}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m.\end{aligned}$$

To see the upper bound, we use $\ell^{3i+1}-1 \geq \frac{1}{2}\ell^{3i+1}$, so that

$$\begin{aligned}\left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \frac{\binom{m}{i}(\ell^2+1)^{m-i}\ell^i}{\ell^{3i+1}-1} &\leq \frac{2}{\ell}\left(\frac{1}{\ell^2+\ell+1}\right)^m \sum_{i=0}^{m} \binom{m}{i}(\ell^2+1)^{m-i}\left(\frac{1}{\ell^2}\right)^i \\ &= \frac{2}{\ell}\left(\frac{\ell^4+\ell^2+1}{\ell^2(\ell^2+\ell+1)}\right)^m,\end{aligned}$$

as claimed.

□

We now consider the product of elliptic curves E_i/F_i such that the image of each torsion representation is the normalizer of a nonsplit Cartan subgroup. As mentioned above, this will occur when each complex multiplication field L_i is not contained in F_i.

Theorem 4.20. *Let $A = E_1 \times E_2 \times \ldots \times E_m$, where for each $i = 1, 2, \ldots, m$, E_i/F_i is an elliptic curve with complex multiplication. Fix a prime $\ell \geq 3$. Suppose we are in the nonsplit case for each E_i and the image of each ρ_i is the full normalizer N_i of a Cartan subgroup C_i. Further, assume the E_i have appropriately intersecting torsion fields and the Kummer map is surjective. Then*

$$\mathcal{F}(G) = \frac{\ell-3}{\ell-1} + \frac{1}{2^m}\sum_{j=0}^{m}\binom{m}{j}\frac{1}{\ell^{j+1}-1} + \frac{1}{2^m(\ell^2+\ell+1)^m}\sum_{i=0}^{m}\binom{m}{i}(2\ell^2+\ell+2)^{m-i}\frac{\ell^i}{\ell^{3i+1}-1}.$$

Proof. Let N be the normalizer of any of the nonsplit Cartan subgroups, C. Let $\bar{N}$ be the reduction of $N \pmod{\ell^n}$ for fixed $n \geq 1$. Define

$$\tilde{r}_{D,k} = \#\{M \in \bar{N} : \det M \equiv D \pmod{\ell^n} \text{ and } \mathrm{ord}_\ell(\det(M-I)) = k\}.$$

Note for $M \in N\backslash C$ that $\det(M-I) = 1 + \det M$. It follows that

$$\tilde{r}_{D,k} = \begin{cases} r_{D,k} + (\ell+1)\ell^{n-1}, & \text{if } k = \operatorname{ord}_\ell(D+1) \\ r_{D,k}, & \text{otherwise,} \end{cases}$$

where $r_{D,k}$ is the quantity defined in Lemma 4.17.

To compute $\mathcal{F}(G)$, consider the function $\tilde{g}_D(x) = \sum_{k=0}^{n} \tilde{r}_{D,k} x^k$ for fixed D and n. Using $\tilde{r}_{D,k}$ described above and $g_D(x)$ defined in the proof of Theorem 4.16, we conclude:

$$\tilde{g}_D\left(\frac{1}{\ell}\right) = g_D\left(\frac{1}{\ell}\right) + \frac{(\ell-1)\ell^{n-1}}{\ell^i},$$

where $i = \operatorname{ord}_\ell(D+1)$.

We know from Proposition 2.8 that

$$\begin{aligned} \mathcal{F}(G) &= \int_{M \in G_{T_\infty/F}} \prod_{i=1}^{m} \ell^{-\operatorname{ord}_\ell(\det(M_i - I))}\, dM \\ &= \lim_{n\to\infty} \sum_{k=0}^{n} \frac{\#\{(M_1,\ldots,M_m) \in G_{T_n/F} : \sum_{i=1}^{m} \operatorname{ord}_\ell(\det(M_i - I)) = k\}}{\ell^k \# G_{T_n/F}} \\ &= \lim_{n\to\infty} \frac{\sum_{D \in (\mathbb{Z}/\ell^n)^\times} \left[\tilde{g}_D\left(\frac{1}{\ell}\right)\right]^m}{(\ell-1)\ell^{n-1}[2(\ell+1)\ell^{n-1}]^m}. \end{aligned}$$

With some computation, it can be shown that the three sums given in the expression for $\mathcal{F}(G)$ in the statement of the theorem correspond to the cases $D \not\equiv -1, 1 \pmod{\ell}$, $D \equiv -1 \pmod{\ell}$, and $D \equiv 1 \pmod{\ell}$, respectively. □

Corollary 4.21. *For $m = 1$,*

$$\mathcal{F}(G) = \frac{2\ell^4 - \ell^3 - \ell^2 - \ell - 2}{\ell^4 - 1}.$$

For $m = 2$,

$$\mathcal{F}(G) = \frac{4\ell^{12} + 5\ell^{11} + \ell^{10} - 8\ell^9 - 20\ell^8 - 27\ell^7 - 32\ell^6 - 35\ell^5 - 36\ell^4 - 32\ell^3 - 23\ell^2 - 11\ell - 4}{4(\ell-1)(\ell+1)(\ell^2+1)(\ell^2+\ell+1)(\ell^6+\ell^5+\ell^4+\ell^3+\ell^2+\ell+1)}.$$

4.5 The General Case

We combine all the results from the previous sections into the following theorem.

Theorem 4.22. *Let A be the product of m elliptic curves E_i with complex multiplication. Fix a prime $\ell \geq 3$. Suppose the image of each torsion representation is a full split Cartan subgroup for m_1 of the curves, is the normalizer of a split Cartan subgroup for m_2 of the curves, is a full nonsplit Cartan subgroup for m_3 curves, and is the normalizer of a nonsplit Cartan subgroup for m_4 of curves, where $m_1 + m_2 + m_3 + m_4 = m$. Further, assume the E_i have appropriately intersecting torsion fields and the Kummer map is surjective. Then*

$$\begin{aligned}\mathcal{F}(G) = &\left(\frac{\ell-3}{\ell-1}\right)\left[\frac{\ell^2-2\ell-1}{\ell^2-1}\right]^{m_1}\left[\frac{\ell^2-\ell-1}{\ell^2-1}\right]^{m_2} \\ &+ \frac{1}{2^{m_2+m4}}\left[\frac{\ell^2-2\ell-1}{\ell^2-1}\right]^{m_1}\sum_{i=0}^{\infty}\frac{1}{\ell^i}\left[\frac{\ell^2-2\ell-1}{\ell^2-1}+\frac{1}{\ell^i}\right]^{m_2}\left[1+\frac{1}{\ell^i}\right]^{m_4} \\ &+ \frac{1}{2^{m_2+m_4}(\ell^3-1)^{m_1+m_2}(\ell^2+\ell+1)^{m_3+m_4}}\left[\sum_{j=1}^{\infty}\frac{1}{\ell^j}\left[\ell^3-\ell^2-\ell-1-\frac{\ell^3+\ell}{\ell^{3j}}\right]^{m_1}\right. \\ &\left.\left[2\ell^3-\ell^2-\ell-2-\frac{\ell^3+\ell}{\ell^{3j}}\right]^{m_2}\left[\ell^2+1+\frac{1}{\ell^{3j-1}}\right]^{m_3}\left[2\ell^2+\ell+2+\frac{1}{\ell^{3j-1}}\right]^{m_4}\right].\end{aligned}$$

Proof. From our work in the previous sections, we have

$$\mathcal{F}(G) = \lim_{n\to\infty}\frac{\sum_{D\in(\mathbb{Z}/\ell^n)^\times}\left[\frac{f_D\left(\frac{1}{\ell}\right)}{(\ell-1)\ell^{n-1}}\right]^{m_1}\left[\frac{\tilde{f}_D\left(\frac{1}{\ell}\right)}{2(\ell-1)\ell^{n-1}}\right]^{m_2}\left[\frac{g_D\left(\frac{1}{\ell}\right)}{(\ell+1)\ell^{n-1}}\right]^{m_3}\left[\frac{\tilde{g}_D\left(\frac{1}{\ell}\right)}{2(\ell+1)\ell^{n-1}}\right]^{m_4}}{(\ell-1)\ell^{n-1}}.$$

The cases $D \not\equiv -1, 1 \pmod{\ell^n}$, $D \equiv -1 \pmod{\ell^n}$, and $D \equiv 1 \pmod{\ell^n}$ correspond to the three respective sums in the expression for $\mathcal{F}(G)$ stated in the theorem. □

Corollary 4.23. *Let $A = E_1 \times E_2$, where E_i is an elliptic curve with complex multiplication. Fix a prime $\ell \geq 3$. Suppose the image of each torsion representation for E_1 is a full split Cartan subgroup and for E_2 is a full nonsplit Cartan subgroup. Further, assume E_1 and E_2 have appropriately intersecting torsion fields and the Kummer map is surjective. Then*

$$\mathcal{F}(G) = \frac{\ell^{13}-\ell^{12}-\ell^{11}-3\ell^{10}+2\ell^8+3\ell^7+4\ell^6+5\ell^5+5\ell^4+7\ell^3+4\ell^2+3\ell+1}{(\ell-1)^2(\ell+1)(\ell^2+1)(\ell^2+\ell+1)(\ell^6+\ell^5+\ell^4+\ell^3+\ell^2+\ell+1)}.$$

Corollary 4.24. *Let $A = E_1 \times E_2$, where E_i is an elliptic curve with complex multiplication. Fix a prime $\ell \geq 3$. Suppose the image of each torsion representation for E_1 is the full normalizer of a split Cartan subgroup and for E_2 is the full normalizer of a nonsplit Cartan subgroup. Further, assume E_1 and E_2 have appropriately intersecting torsion fields and the Kummer map*

is surjective. Then

$$\begin{aligned}\mathcal{F}(G) = \quad & [4\ell^{14} + \ell^{13} - 5\ell^{12} - 13\ell^{11} - 13\ell^{10} - 2\ell^9 + 10\ell^8 \\ & + 17\ell^7 + 24\ell^6 + 29\ell^5 + 37\ell^4 + 37\ell^3 + 27\ell^2 + 15\ell + 4] \ / \\ & [4(\ell-1)^2(\ell+1)^2(\ell^2+1)(\ell^2+\ell+1)(\ell^6+\ell^5+\ell^4+\ell^3+\ell^2+\ell+1)].\end{aligned}$$

Corollary 4.25. *Let $A = E_1 \times E_2 \times E_3 \times E_4$, be a product of four elliptic curves with complex multiplication. Fix $\ell \geq 3$. Assume the torsion representation for the E_i are one of each different type listed in Theorem 4.22. Further, assume the E_i having appropriately intersecting torsion fields and the Kummer map is surjective. Then*

$$\begin{aligned}\mathcal{F}(G) = \quad & [4\ell^{38} + \ell^{37} - 9\ell^{36} - 30\ell^{35} - 21\ell^{34} + 38\ell^{33} + 148\ell^{32} + 260\ell^{31} + 335\ell^{30} + 316\ell^{29} \\ & + 198\ell^{28} - 58\ell^{27} - 440\ell^{26} - 977\ell^{25} - 1628\ell^{24} - 2385\ell^{23} - 3194\ell^{22} - 4038\ell^{21} \\ & - 4890\ell^{20} - 5706\ell^{19} - 6427\ell^{18} - 6980\ell^{17} - 7299\ell^{16} - 7375\ell^{15} - 7205\ell^{14} - 6850\ell^{13} \\ & - 6323\ell^{12} - 5670\ell^{11} - 4906\ell^{10} - 4078\ell^9 - 3244\ell^8 - 2452\ell^7 - 1745\ell^6 - 1135\ell^5 \\ & - 655\ell^4 - 314\ell^3 - 119\ell^2 - 31\ell - 4] \ / \\ & [4(\ell+1)^2(\ell^2+1)(\ell^2+\ell+1)^2(\ell^7-1)(\ell^{10}-1)(\ell^{13}-1)]\end{aligned}$$

CHAPTER 5

ABELIAN SURFACES WITH REAL MULTIPLICATION

5.1 Preliminaries and Past Work

Let A be an abelian variety of dimension $d > 1$ defined over a global field F. The Galois invariance and non-degeneracy of the Weil pairing $e_{\ell^n} : A[\ell^n] \times \hat{A}[\ell^n] \to \mu_{\ell^n}$ implies that $\mathrm{im}\rho_{\ell^n} \subseteq \mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n)$, the group of symplectic similitudes. In [10], Jones and Rouse find necessary and sufficient conditions for when $\mathrm{im}\rho_{\ell^n}$ is all of $\mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n)$.

Proposition 5.1 ([10, Proposition 6.1], [26, Theorems 4.1, 4.2.1])**.** *Let ℓ be a prime and $d \geq 2$. Then, the ℓ-adic representation $\rho : G_{T_\infty/F} \to GSp_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if the following conditions hold:*

(i) F is linearly disjoint from $\mathbb{Q}(\zeta_n)$ for all n;

(ii) $G_{T_1/F} \cong GSp_{2d}(\mathbb{Z}/\ell)$;

(iii) if $\ell = d = 2$, then T_1 is linearly disjoint from $\mathbb{Q}(\sqrt{2}, i)$.

Remark 5.2 ([10, Remark, p. 23])**.** In the case when d is odd, $d = 2$, or $d = 6$, and $\mathrm{End}(A) \cong \mathbb{Z}$, by [21, Théorème 3], the above conditions are applicable for ℓ sufficiently large.

Under the assumptions above, Jones and Rouse determine necessary and sufficient conditions for when the Kummer map is surjective.

Proposition 5.3 ([10, Theorem 6.2])**.** *Let ℓ be a prime and $d \geq 2$. Assume the ℓ-adic representation $\rho : G_{T_\infty/F} \to GSp_{2d}(\mathbb{Z}_\ell)$ is surjective. Then the Kummer map $\kappa : G_{K_\infty/T_\infty} \to \mathbb{Z}_\ell^{2d}$ is surjective if and only if the following conditions hold:*

(i) $\alpha \notin \ell A(F)$;

(ii) if $\ell = 2$, then $\beta_1 \notin A(T_1)$.

The two propositions above give the following corollary.

Corollary 5.4 ([10, Corollary 6.3])**.** *The arboreal representation $\omega : G_{K_\infty/F} \to \mathbb{Z}_\ell^{2d} \rtimes GSp_{2d}(\mathbb{Z}_\ell)$ is surjective if and only if Propositions 5.1 and 5.3 are satisfied.*

In the case of surjective arboreal representation above, Jones and Rouse are unable to use their previous methods to compute the density $\mathcal{F}(G)$. Even in the abelian surface case (so $d = 2$), the image of ρ as a subgroup of $\mathrm{GSp}_4(\mathbb{Z}_\ell)$ is much too large to compute the integral in Proposition 2.8. By utilizing a computation from [12, p. 61] of the number of $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ with $\det(M - I) \not\equiv 0 \pmod{\ell}$, Jones and Rouse determine the bounds:

$$\frac{\ell^7 - 2\ell^6 - \ell^5 + 4\ell^4 - 2\ell^3 + 2\ell^2 - 5}{(\ell^4 - 1)(\ell^2 - 1)(\ell - 1)} \leq \mathcal{F}(G) \leq \frac{\ell^7 - \ell^6 - \ell^5 + 3\ell^4 - 2\ell^3 + \ell^2 - 4}{\ell^7 - \ell^5 - \ell^3 + \ell}.$$

In this chapter, we examine the $d = 2$ case in which the image of ρ is not all of $\mathrm{GSp}_4(\mathbb{Z}_\ell)$. Specifically, we consider abelian surfaces with real multiplication by the ring of integers $\mathcal{O}$ of a quadratic field F. Let $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$ and set $\mathcal{O}_\ell = \mathbb{Z}_\ell[\omega], \omega^2 \in \mathbb{Z}_\ell$. Define

$$H = \{M \in \mathrm{GL}_2(\mathcal{O}_\ell) : \det(M) \in \mathbb{Z}_\ell^\times\},$$

which injects into $\mathrm{Aut}(T_\ell(A)) \cong \mathrm{GL}_4(\mathbb{Z}_\ell)$ via the map

$$\begin{bmatrix} a_1 + a_2\omega & b_1 + b_2\omega \\ c_1 + c_2\omega & d_1 + d_2\omega \end{bmatrix} \longmapsto \begin{bmatrix} a_1 & a_2\omega^2 & b_1 & b_2\omega^2 \\ a_2 & a_1 & b_2 & b_1 \\ c_1 & c_2\omega^2 & d_1 & d_2\omega^2 \\ c_2 & c_1 & d_2 & d_1 \end{bmatrix}.$$

Theorem 2.14 says that $G_{T_\infty/F}$ is isomorphic to a subgroup of H, and is isomorphic to all of H for almost all ℓ. In the case where ρ surjects onto H, we determine necessary and sufficient conditions for when the Kummer map is be surjective and compute the density $\mathcal{F}(G)$.

5.2 Conclusions

We begin with the following proposition, which gives necessary and sufficient conditions for when the Kummer map is surjective.

Proposition 5.5. *Let A be an Abelian surface defined over $\mathbb{Q}$ and let F be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}$. Fix an inert prime $\ell > 2$. Let $\mathcal{O}_\ell = \mathcal{O} \otimes \mathbb{Z}_\ell$ and set $\mathcal{O}_\ell = \mathbb{Z}_\ell[\omega]$, $\omega^2 \in \mathbb{Z}_\ell$. Assume $G_{T_\infty/\mathbb{Q}} \cong \{M \in GL_2(\mathcal{O}_\ell) : det(M) \in \mathbb{Z}_\ell^\times\}$. Then the Kummer map $\kappa : G_{K_\infty/T_\infty} \to \mathbb{Z}_\ell^4$ is surjective if and only if $\alpha \notin \ell A(F)$.*

Proof. The only if part of the statement is clear since if $\alpha \in \ell A(F)$, then κ cannot be surjective.

To see the converse, assume $\alpha \notin \ell A(F)$. Then $J = \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in (\mathbb{Z}_\ell/\ell)^\times\}$ has order $\ell - 1$ and is thus a normal subgroup of $G_{T_1/\mathbb{Q}}$ with order coprime to ℓ. Since $A[\ell]^J = 0$, Proposition 2.7 implies that $A(\mathbb{Q}) \cap \ell A(T_1) = \ell A(\mathbb{Q})$.

Next, $N^{(n)}/N^{(n+1)}$ is isomorphic to the subgroup of $M_2(\mathcal{O}_\ell/\ell)$ with conjugate elements along the main diagonal as a $G_{T_1/\mathbb{Q}}$-module with the conjugation action. Since $G_{T_1/\mathbb{Q}}$ contains the matrix $\left(\begin{smallmatrix} -1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, which acts trivially on $N^{(n)}/N^{(n+1)}$, but acts as multiplication by -1 on $A[\ell]$, we have

$$\mathrm{Hom}_{G_{T_1/\mathbb{Q}}}(N^{(n)}/N^{(n+1)}, A[\ell]) = 0.$$

Proposition 2.6 now implies that $A(\mathbb{Q}) \cap \ell A(T_n) = A(\mathbb{Q}) \cap \ell A(T_{n+1})$.

We now show $A[\ell]$ is irreducible as a $G_{T_1/\mathbb{Q}}$-module over $\mathbb{Z}_\ell/\ell$. Certainly, it is irreducible as a $G_{T_1/\mathbb{Q}}$-module over $\mathcal{O}_\ell/\ell$, since the matrices $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ are in $G_{T_1/\mathbb{Q}}$ and do not share an eigenvector. Now suppose there is a non-zero submodule N of $A[\ell]$ that is $G_{T_1/\mathbb{Q}}$-invariant over $\mathbb{Z}_\ell/\ell$. Then, in particular, the matrix $W = \left(\begin{smallmatrix} \omega & 0 \\ 0 & \omega \end{smallmatrix}\right) \in G_{T_1/\mathbb{Q}}$ preserves N. For all $a + b\omega \in \mathcal{O}_\ell/\ell$, all $M \in G_{T_1/\mathbb{Q}}$, and all $x \in N$, we then have $M.(a + b\omega)x = (aM).x + (bMW).x \in N$. Hence, N is irreducible when viewed as a $G_{T_1/\mathbb{Q}}$-module over $\mathcal{O}_\ell/\ell$. We conclude $N = A[\ell]$ and thus that $A[\ell]$ is irreducible as a $G_{T_1/\mathbb{Q}}$ module over $\mathbb{Z}_\ell/\ell$. Proposition 2.5 now implies that $\mathrm{im}\omega_n \cong A[\ell] \rtimes G_{T_n/\mathbb{Q}}$ for all $n \geq 1$.

□

We therefore have the following corollary.

Corollary 5.6. *Let A, F, ℓ, and $\mathcal{O}_\ell$ be as in Proposition 5.5 and fix $\alpha \notin \ell A(F)$. Then for almost all ℓ, the arboreal representation $\omega : G_{K_\infty/F} \longrightarrow \mathcal{O}_\ell^2 \rtimes H$ is surjective for almost all ℓ.*

We can now compute $\mathcal{F}(G)$.

Proposition 5.7. *Let A be an Abelian surface defined over $\mathbb{Q}$ and let F be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}$. Let ℓ be an inert prime and define $R_n = \mathcal{O}_\ell/(\ell^n)$. Let $R = \varprojlim R_n$.*

Assume the ℓ-adic Kummer map κ is surjective and the torsion part, imρ as a subset of $GL_4(\mathbb{Z}_\ell)$ is isomorphic to $H = \{M \in GL_2(R) : det(M) \in \mathbb{Z}_\ell^\times\}$. Then

$$\mathcal{F}(G) = \int_H \ell^{-ord'_\ell(det(M-I))} d\mu$$

where $d\mu$ denotes the Haar measure on H, normalized so $\mu(H) = 1$ and ord'_ℓ is such that $ord'_\ell(\ell) = 2$ and $ord'_\ell(0) = \infty$.

Proof. Since κ is surjective, by Proposition 2.8, we have

$$\mathcal{F}(G) = \int_{\mathrm{im}\rho} \ell^{-\mathrm{ord}_\ell(\det(M-I))} d\mu$$

where $d\mu$ denotes the Haar measure on imρ, normalized so $\mu(\mathrm{im}\rho) = 1$ and ord_ℓ is such that $\mathrm{ord}_\ell(\ell) = 1$ and $\mathrm{ord}_\ell(0) = \infty$. We must determine how ord_ℓ changes when we use the isomorphism $\mathrm{im}\rho \cong H$.

Write $\mathcal{O} = \mathbb{Z}_\ell[\omega]$ where $\omega^2 \in \mathbb{Z}_\ell$. We include H into $\mathrm{GL}_4(\mathbb{Z}_\ell)$ via the map

$$M' = \begin{bmatrix} a_1 + a_2\omega & b_1 + b_2\omega \\ c_1 + c_2\omega & d_1 + d_2\omega \end{bmatrix} \longmapsto M = \begin{bmatrix} a_1 & a_2\omega^2 & b_1 & b_2\omega^2 \\ a_2 & a_1 & b_2 & b_1 \\ c_1 & c_2\omega^2 & d_1 & d_2\omega^2 \\ c_2 & c_1 & d_2 & d_1 \end{bmatrix}.$$

Note this map is clearly injective, since if $M = I$, then $a_1 = d_1 = 1$ and $a_2 = b_1 = b_2 = c_1 = c_2 = d_2 = 0$.

We now compare $\det(M - I)$ and $\det(M' - I)$. Let $\det(M') = s$. Since $s \in \mathbb{Z}_\ell^\times$, we have $a_1d_2 + a_2d_1 - b_1c_2 - b_2c_1 = 0$. Thus $\det(M' - I) = a_1d_1 - a_1 - d_1 + 1 - b_1c_1 + a_2d_2\omega^2 - b_2c_2\omega^2 - (a_2+d_2)\omega = s - a_1 - d + 1 - (a_2+d_2)\omega$. On the other hand, write $M - I$ as the block matrix $\left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$. It is a common linear algebra fact that since C and D commute, $\det(M - I) = \det(AD - BC)$. Using $a_1d_2 + a_2d_1 - b_1c_2 - b_2c_1 = 0$, we have

$$AD - BC = \begin{bmatrix} \det(M' - I) + (a_2 + d_2)\omega & -(a_2 + d_2)\omega^2 \\ -(a_2 + d_2) & \det(M' - I) + (a_2 + d_2)\omega \end{bmatrix}.$$

We conclude $\det(M - I) = [(s - a_1 - d_1 + 1) - (a_2 + d_2)\omega][(s - a_1 - d_1 + 1) + (a_2 + d_2)\omega] = \det(M' - I)\overline{\det(M' - I)}$. Our result now follows. □

Theorem 5.8. *Let A be an abelian surface defined over $\mathbb{Q}$ and let F be a quadratic extension of $\mathbb{Q}$ with ring of integers $\mathcal{O}$. Let ℓ be an inert prime and define $R_n = \mathcal{O}_\ell/(\ell^n)$. Let $R = \varprojlim R_n$. Assume $im\rho \cong \{M \in GL_2(R) : det(M) \in \mathbb{Z}_\ell^\times\}$ and fix $\alpha \notin \ell A(F)$ so that the Kummer map is surjective. Then*

$$\mathcal{F}(G) = \frac{\ell^{15} - \ell^{13} - \ell^{11} + \ell^{10} + \ell^9 + \ell^3 + \ell^2 + 1}{\ell^{15} - \ell^{11} - \ell^4 + 1}.$$

Proof. For

$$G_{T_n/\mathbb{Q}} \cong \{M \in \mathrm{GL}_2(R_n) : \det(M) \in (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times\}$$

consider the subset

$$C_n = \{M \in G_{T_n/\mathbb{Q}} : \det(M - I) \equiv 0 \pmod{\ell^{n-1}} \text{ but } \det(M - I) \not\equiv 0 \pmod{\ell^n}\}.$$

and set $c_n = \#C_n$. Since $\mu(C_n) = \frac{c_n}{\#G_{T_n/\mathbb{Q}}}$ and $\mathrm{ord}_\ell(\det(M - I)) = 2(n-1)$ for all M in C_n, by Proposition 5.7, the density $\mathcal{F}(G)$ can be computed by evaluating the sum

$$\mathcal{F}(G) = \sum_{n=1}^{\infty} \frac{c_n}{\ell^{2(n-1)}\#G_{T_n/\mathbb{Q}}}.$$

We first compute $c_1 = \#\{M \in G_{T_1/\mathbb{Q}} : \det(M - I) \not\equiv 0 \pmod{\ell}\}$. Let $M = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$. Then we want to count the number of $(a, b, c, d, s) \in R_1^4 \times (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$ such that $ad - bc \equiv s$ and $s - a - d + 1 \not\equiv 0 \pmod{\ell}$. We analyze two cases.

First, assume $b \not\equiv 0 \pmod{\ell}$. Then b is a unit and we have $c \equiv (ad - s)b^{-1} \pmod{\ell}$. Note that if d is any element of $R_1 \cong \mathbb{F}_{\ell^2}$ and s any element of $(\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$, then we can choose any $a \not\equiv d - 1 - s \pmod{\ell}$. We therefore have $(\ell^2 - 1)\ell^2(\ell - 1)(\ell^2 - 1) = \ell^2(\ell^2 - 1)^2(\ell - 1)$ matrices in this case.

If $b \equiv 0 \pmod{\ell}$, then c can be any element and a and d are both units such that $ad \in (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$. Further, since we need $s - a - d + 1 \equiv (a - 1)(d - 1) \pmod{\ell}$ to be nonzero, we must have $a \not\equiv 1 \pmod{\ell}$ and $d \not\equiv 1 \pmod{\ell}$. If $d \in (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$, then choosing $a \not\equiv 1 \pmod{\ell}$ and $d \not\equiv 1 \pmod{\ell}$ satisfies all our requirements. There are therefore $\ell^2(\ell - 2)^2$ matrices in this case. If $d \notin (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$ and $ad \equiv s \in (\mathbb{Z}_\ell/\ell\mathbb{Z}_\ell)^\times$, then $a \equiv d^{-1}s \not\equiv 1 \pmod{\ell}$ for any s. There are then $\ell^2(\ell^2 - \ell)(\ell - 1) = \ell^3(\ell - 1)^2$ matrices in this case.

Adding all of these cases together, we obtain $c_1 = \ell^7 - \ell^6 - \ell^5 + \ell^4 - 2\ell^3 + 3\ell^2$.

To find c_n recursively for $n \geq 2$, we use the following lemma.

Lemma 5.9. *For $n \geq 1$ define*

$$d_n = \#\{(a, b, c, s) \in R_n^3 \times \mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell : bc \equiv (s - a)a \ (mod\ \ell^n)\}.$$

Set $d_{-1} = \ell^{-7}$. Then for $n \geq 1$,

$$d_n = \ell^{5n-5}(\ell^5 + \ell^3 - \ell^2 - 1) + \ell^7 d_{n-2}.$$

Proof. A little computation gives us that $d_0 = 1$ and $d_1 = \ell^2(\ell^3 + \ell - 1)$ so that d_1 satisfies the specified recursion relation. We now show it for $n \geq 2$.

If b is a unit, then c is determined, whereas a and s can be any elements of R_n and $\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell$, respectively. There are thus $\ell^{5n-2}(\ell^2 - 1)$ such tuples.

Now assume b is not a unit, but s is. Then the polynomial equation $bc = (s - x)x$ has two distinct solutions (mod ℓ), namely $x \equiv 0 \pmod{\ell}$ and $x \equiv s \pmod{\ell}$. By Hensel's Lemma, this polynomial has a unique solution (mod ℓ^n) for each of our two (mod ℓ) solutions. Since c was arbitrary in this process, we conclude there are $2\ell^{5n-3}(\ell - 1)$ tuples in this case.

We now suppose b and s are nonunits, but c is a unit. Note then a must also be a nonunit. We then have $b \equiv (s - a)ac^{-1} \pmod{\ell^n}$, so there are $\ell^{5n-5}(\ell^2 - 1)$ tuples in this case.

Finally, suppose b, s, and c are nonunits, which implies a is also a nonunit. Letting $a = a'\ell$, $b = b'\ell$, $c = c'\ell$, and $s = s'\ell$, where $(a', b', c', s') \in R_{n-1}^3 \times \mathbb{Z}_\ell/\ell^{n-1}\mathbb{Z}_\ell$, we have the condition $bc \equiv (s - a)a \pmod{\ell^n}$ is equivalent to the condition $b'c' \equiv (s' - a')a' \pmod{\ell^{n-2}}$. Since d_{n-2} gives the number of solutions in $R_{n-2}^3 \times \mathbb{Z}_\ell/\ell^{n-2}\mathbb{Z}_\ell$, we lift each solution to (mod ℓ^{n-1}) solutions to obtain $\ell^7 d_{n-2}$ tuples in this case.

We have therefore found that for $n \geq 2$, $d_n = \ell^{5n-5}(\ell^5 + \ell^3 - \ell^2 - 1) + \ell^7 d_{n-2}$, as claimed. □

We now compute c_n for $n \geq 2$. This is equivalent to counting all $(a, b, c, d, s, t) \in R_n^4 \times (\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times \times R_1^\times$ such that $ad - bc \equiv s \pmod{\ell^n}$ and $s - a - d + 1 \equiv t\ell^{n-1} \pmod{\ell^n}$. We again consider various cases.

First, if b is a unit, then $c \equiv (ad - s)b^{-1} \pmod{\ell}$, where we are free to choose d, s, and t and have $a \equiv s - d + 1 + t\ell^{n-1} \pmod{\ell}$. There are therefore $\ell^{5n-3}(\ell^2 - 1)^2(\ell - 1)$ tuples in this case.

If b is not a unit, then a and d must be units and we have $d \equiv (bc + s)a^{-1} \pmod{\ell}$. Plugging this into our second condition and multiplying by a gives $a^2 - (s + 1 + t\ell^{n-1})a + s + bc \equiv 0 \pmod{\ell^n}$. Since the polynomial $x^2 - (s + 1 + t\ell^{n-1})x + s + bc$ has roots $x \equiv s \pmod{\ell}$ and $x \equiv 1 \pmod{\ell}$, if we assume $s \not\equiv 1 \pmod{\ell}$, then by Hensel's Lemma, each solution lifts to a unique solution (mod ℓ^n). Since c was arbitrary in this process, we conclude that there are $2\ell^{5n-3}(\ell^2 - 1)(\ell - 2)$ tuples in this case.

We now assume b is not a unit and $s \equiv 1 \pmod{\ell}$. Then a and d are also congruent to 1 (mod ℓ). Further, assume c is a unit. Then a and b are fixed and d can be any unit. We therefore have $\ell^{5n-5}(\ell^2-1)^2$ tuples in this case.

This exhausts all possible cases when $n = 2$, so for the last case, assume $n \geq 3$. Let b and c be nonunits and a, d, $s \equiv 1 \pmod{\ell}$. Note d is fixed: $d \equiv (bc+s)a^{-1} \pmod{\ell^n}$. Plugging this into our second condition, we see that we want to find (a, b, c, s) such that $bc \equiv (s-a)(a-1) \pmod{\ell^{n-1}}$ but $bc \not\equiv (s-a)(a-1) \pmod{\ell^n}$. Write $a = a'\ell + 1$, $b = b'\ell$, $c = c'\ell$, $s = s'\ell + 1$, where $(a, b, c, s) \in R_{n-1}^3 \times \mathbb{Z}_\ell/\ell^{n-1}\mathbb{Z}_\ell$. Then plugging this into the above relation, we have our condition is equivalent to $b'c' \equiv (s'-a')a' \pmod{\ell^{n-3}}$ but $b'c' \not\equiv (s'-a')a' \pmod{\ell^{n-2}}$. The number of $(a', b', c', s') \in R_{n-3}^3 \times \mathbb{Z}_\ell/\ell^{n-3}\mathbb{Z}_\ell$ satisfying the first of these conditions is d_{n-3}. We lift to (mod ℓ^{n-2}) and subtract the number of these that satisfy the second condition (which is d_{n-2}) to obtain $\ell^7 d_{n-3} - d_{n-2}$. Finally, we lift these to (mod ℓ^{n-1}) solutions to obtain $\ell^{14}d_{n-3} - \ell^7 d_{n-2}$ tuples in this case. Note that by defining $d_{-1} = \ell^{-7}$, we get 0 for the above expression if we plug in $n = 2$, allowing us to conclude that for all $n \geq 2$,

$$c_n = \ell^{5n-5}(\ell^2-1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1) + \ell^{14}d_{n-3} - \ell^7 d_{n-2}.$$

Using the recursion relation $\ell^7 d_{n-2} = d_n - \ell^{5n-5}(\ell^5 + \ell^3 - \ell^2 - 1)$ from Lemma 5.9 twice, we obtain the following recursion for c_n for $n \geq 2$:

$$c_n = \frac{1}{\ell^7}c_{n+2} + \ell^{5n-12}(\ell^2-1)(\ell^7-1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1) - \ell^{5n-5}(\ell^7-1)(\ell^5 + \ell^3 - \ell^2 - 1).$$

We now compute $\mathcal{F}(G)$. Note that since $\det{:}\mathrm{GL}_2(R_n) \to R_n^\times$ is a surjectve group homomorphism, we have

$$\#G_{T_n/\mathbb{Q}} = \frac{\#\mathrm{GL}_2(R_n)}{\#R_n^\times} \cdot \#(\mathbb{Z}_\ell/\ell^n\mathbb{Z}_\ell)^\times = \ell^{7n-5}(\ell^4-1)(\ell-1).$$

We therefore have

$$
\begin{aligned}
\mathcal{F}(G) &= \sum_{n=1}^{\infty} \frac{c_n}{\ell^{2(n-1)} \# G_{T_n/\mathbb{Q}}} \\
&= \frac{\ell^5 - \ell^4 - \ell^3 + \ell^2 - 2\ell + 3}{(\ell^4 - 1)(\ell - 1)} + \sum_{n=2}^{\infty} \frac{\frac{1}{\ell^7} c_{n+2}}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} \\
&+ \sum_{n=2}^{\infty} \frac{\ell^{5n-12}(\ell^2 - 1)(\ell^7 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} - \sum_{n=2}^{\infty} \frac{\ell^{5n-5}(\ell^7 - 1)(\ell^5 + \ell^3 - \ell^2 - 1)}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} \\
&= \frac{\ell^5 - \ell^4 - \ell^3 + \ell^2 - 2\ell + 3}{(\ell^4 - 1)(\ell - 1)} + \ell^{11} \sum_{n=4}^{\infty} \frac{c_n}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} \\
&+ \sum_{n=2}^{\infty} \frac{\ell^{5n-12}(\ell^2 - 1)(\ell^7 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} - \sum_{n=2}^{\infty} \frac{\ell^{5n-5}(\ell^7 - 1)(\ell^5 + \ell^3 - \ell^2 - 1)}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} \\
&= \frac{\ell^5 - \ell^4 - \ell^3 + \ell^2 - 2\ell + 3}{(\ell^4 - 1)(\ell - 1)} + \ell^{11} \mathcal{F}(G) - \ell^{11} \sum_{n=1}^{3} \frac{c_n}{\ell^{9n-7}(\ell^4 - 1)(\ell - 1)} \\
&+ \frac{(\ell^7 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{(\ell - 1)(\ell^2 + 1)} \sum_{n=2}^{\infty} \frac{1}{\ell^{4n+5}} - \frac{(\ell^7 - 1)(\ell^2 + \ell + 1)}{\ell^2 - 1} + \sum_{n=2}^{\infty} \frac{1}{\ell^{4n+2}} \\
&= \ell^{11} \mathcal{F}(G) - (\ell^{11} - 1) \frac{\ell^5 - \ell^4 - \ell^3 + \ell^2 - 2\ell + 3}{(\ell^4 - 1)(\ell - 1)} \\
&- \ell^{11} \left(\frac{\ell^5(\ell^2 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{\ell^{11}(\ell^4 - 1)(\ell - 1)} - \frac{\ell^{10}(\ell^2 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{\ell^{20}(\ell^4 - 1)(\ell - 1)} \right) \\
&+ \frac{(\ell^7 - 1)(\ell^5 - \ell^4 + \ell^3 - 2\ell^2 - 1)}{\ell^9(\ell - 1)(\ell^2 + 1)(\ell^4 - 1)} - \frac{(\ell^7 - 1)(\ell^2 + \ell + 1)}{\ell^6(\ell^2 - 1)(\ell^4 - 1)}.
\end{aligned}
$$

Solving for $\mathcal{F}(G)$, we obtain:

$$
\mathcal{F}(G) = \frac{\ell^{15} - \ell^{13} - \ell^{11} + \ell^{10} + \ell^9 + \ell^3 + \ell^2 + 1}{\ell^{15} - \ell^{11} - \ell^4 + 1}.
$$

□

5.3 An Example

The goal of this section is to provide an example of an abelian surface A with real multiplication that satisfies the conditions of Theorem 5.8 for all primes ℓ inert in the real quadratic multiplication field of A.

Consider $A = J_0(23)$, the Jacobian variety of $X_0(23) = \mathfrak{H}\widehat{\backslash \Gamma_0(23)}$. We find the corresponding newforms. Eichler-Shimura theory gives us that the $\mathbb{Q}$-isogeny factors of $J_0(p)$ corresponds to the the $\mathbb{Q}$-conjugacy classes of modular forms of level p and the dimension of each factor corresponds

to the size of the conjugacy class. One can check that A is of genus two. Since there are no elliptic curves over $\mathbb{Q}$ of conductor 23, A has no one dimensional factor. Thus A is an abelian surface and there are two basis elements, f_1, f_2, that are modular forms of level 23 with integer coefficients. Using SAGE (see Appendix A), we obtain:

$$f_1 = q - q^3 - q^4 - 2q^6 + 2q^7 - q^8 + 2q^9 + O(q^{10}) \text{ and}$$
$$f_2 = q^2 - 2q^3 - q^4 + 2q^5 + q^6 + 2q^7 - 2q^8 + O(q^{10})$$

Using the Hecke action, $a_n(T_p(f)) = a_{np}(f)$ for $p \not| n$ and $a_n(T_p(f)) = a_{np}(f) + p a_{\frac{n}{p}}(f)$ for $p|n$, we find the newform $f = f_1 + \frac{-1+\sqrt{5}}{2} f_2$ and its conjugate. Since f has coefficients in $\mathbb{Q}(\sqrt{5})$, we have that A is an abelian surface with real multiplication with real multiplication field $\mathbb{Q}(\sqrt{5})$.

Theorem 2.14 tells us that ρ surjectives onto $H = \{M \in \mathrm{GL}_2(R) : \det(M) \in \mathbb{Z}_\ell^\times\}$ for almost all ℓ. Our goal then is to obtain an effective version of this result for our choice of A by determining an explicit list of the exceptional ℓ. By analyzing all possible maximal subgroups of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ from Section 2.5, we obtain the following result.

Theorem 5.10. *Let $A = J_0(23)$. Then for all $\ell > 5$ inert in $\mathbb{Q}(\sqrt{5})$ there exists a quadratic twist A_d of A and $\alpha \in A_d$ satisfying the conditions of Theorem 5.8. Thus, the density of primes p for which the order of α (mod p) is not divisible by ℓ is $\frac{\ell^{15}-\ell^{13}-\ell^{11}+\ell^{10}+\ell^9+\ell^3+\ell^2+1}{\ell^{15}-\ell^{11}-\ell^4+1}$.*

Let G be the image of ρ and G_ℓ the image of G (mod ℓ). We use the results of Ribet [[17], page 192] to determine the possible exceptional G. We have ρ is surjective whenever the following conditions hold:

1. the determinant map $G \longrightarrow \mathbb{Z}_\ell^\times$ is surjective
2. $\ell \geq 5$
3. G contains an element x_ℓ such that (trace x)^2 generates $\mathbb{Q}_\ell(\sqrt{5})$
4. G_ℓ is an irreducible subgroup of $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$ whose order is divisible by ℓ.

Proof. We first note that if ρ surjects onto H, then the torsion representation ρ' of any quadratic twist A_d of A also surjects onto H. Indeed, since $\rho' = \rho \otimes \left(\frac{d}{\cdot}\right)$, either im$\rho'$ is all of H or an index two subgroup of H. If the latter case were possible, then its determinant one subgroup would give an index two subgroup of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$. But consulting the list of possible subgroups of $\mathrm{SL}_2(\mathbb{F}_{\ell^2})$ in

Section 2.5, we see no such subgroup exists. Thus, $\text{im}\rho' = H$. By [11], [16], and [2], there exists a quadratic twist of A with rank one. We can therefore always find A_d and $\alpha \in A_d(\mathbb{Q})$ such that A_d has surjective ℓ-adic torsion representation and $\alpha \notin \ell A_d(\mathbb{Q})$, as desired. Hence, all there is left to prove is ρ surjects onto H for all $\ell > 5$ inert in $\mathbb{Q}(\sqrt{5})$.

Suppose G is exceptional for a particular $\ell > 5$. Then G fails to satisfy the four criteria for surjective ρ listed above. Note that criterion 1 is always true and since $a_5(f) = -1 + \sqrt{5}$, we may choose x_ℓ in criterion 3 to be $\rho_\ell(\text{Frob}_5)$ for all $\ell \neq 2$. We are left to examine criterion 4. Using the list from Section 2.5, we see that the only possible irreducible subgroups divisible by ℓ are the subfield subgroups. We therefore aim to show that for our given newform f, the determinant one subgroup of G_ℓ cannot be a subfield subgroup for $\ell > 5$ inert in $\mathbb{Q}(\sqrt{5})$.

Suppose $K = G_\ell \cap \text{SL}_2(\mathbb{F}_{\ell^2})$ is a subfield subgroup. Then $K \subseteq \text{SL}_2(\mathbb{F}_{\ell^2})$ has an index two normal subgroup $S \cong \text{SL}_2(\mathbb{F}_\ell)$. Let $J \subseteq \text{GL}_2(\mathbb{F}_{\ell^2})$ be the subgroup of scalar matrices. Note that $J \cap K = \{\pm I\}$. Using that $G_\ell \cdot \text{SL}_2(\mathbb{F}_{\ell^2}) \subseteq \text{GL}_2(\mathbb{F}_{\ell^2})$, we have

$$\begin{aligned}\frac{|G_\ell|}{|G_\ell \cap \text{SL}_2(\mathbb{F}_{\ell^2})|} &\leq \frac{|\text{GL}_2(\mathbb{F}_{\ell^2})|}{|\text{SL}_2(\mathbb{F}_{\ell^2})|} \\ &= \ell^2 - 1\end{aligned}$$

Noting that $G_\ell \cap \text{SL}_2(\mathbb{F}_{\ell^2}) = K$ and multiplying both sides of the above inequality by $\frac{|J \cap K|}{|J|} = \frac{2}{\ell^2 - 1}$, we have

$$\begin{aligned}2 &\geq \frac{|G_\ell||J \cap K|}{|J||K|} \\ &= \frac{|G_\ell|}{|JK|}\end{aligned}$$

We therefore have that JK has index at most two in G_ℓ. It follows that JS has index at most four in G_ℓ.

For a prime p, let $M = \rho_\ell(\text{Frob}_p)$. Then $\text{tr}M = a_p(f)$ and $\det M = p$. Using $\text{tr}M^2 = (\text{tr}M)^2 - 2p$, it can be shown that

$$\text{tr}M^4 = a_p(f)^4 - 4pa_p^2 + 2p^2.$$

On the other hand, by the argument above, $M^4 \in JS$, so that $\text{tr}M^4 = tm$, $t \in \mathbb{F}_{\ell^2}^\times$ and $m \in \mathbb{F}_\ell$. But since $p^4 = \det M^4 = t^2$, we have $t = \pm p^2 \in \mathbb{F}_\ell$. We have then that for all p

$$a_p(f)^4 - 4pa_p^2 + 2p^2 \in \mathbb{F}_\ell.$$

Using the SAGE computation in Appendix A, we find $a_{11} = -3 - \sqrt{5}$. Thus, letting $p = 11$, we have $a_p(f)^4 - 4pa_p^2 + 2p^2 = 2 - 96\sqrt{5}$, which is not in $\mathbb{F}_\ell$ for all $\ell > 3$. We conclude ρ is surjective. Our result now follows. $\square$

CHAPTER 6

FUTURE WORK

6.1 Reducible Elliptic Curves

6.1.1 The cases $\ell = 2$ and $\ell = 3$

One of my immediate goals is to analyze the results of my thesis for the $\ell = 2, 3$ cases for reducible elliptic curves and the $\ell = 2$ case for abelian surfaces with real multiplication. The latter is of particular interest, since for an abelian surface A, the multiplication by two map defines an endomorphism of the Kummer surface obtained by resolving the singularities of $A/\pm 1$. This gives us a new class of surfaces to study the arithmetic dynamics of. Specifically, we may explore the possibility of using the local information involving periodic points mod $\mathcal{P}$ to uncover whether or not global periodic points exist.

The main difficulty in the small ℓ cases is determining the possible images of the arboreal representation. This is directly related to the added complexity in computing the cohomology groups $H^1(G_{T_n/F}, A[\ell])$, which can be larger and harder to describe for small ℓ. For A an abelian surface with real multiplication, I have computed $\mathcal{F}(G)$ in the $\ell = 2$ case under the assumption that the Kummer map is surjective. Thus, all that is left to determine are necessary and sufficient conditions for when the Kummer map is surjective for $\ell = 2$. This hinges upon uncovering when the cohomology groups $H^1(G_{T_n/F}, A[2])$ vanish. For $\ell = 2$, the condition that $\alpha \notin \ell A(\mathbb{Q})$ is not sufficient. For example, if $F(\beta_1) \subset F(A[4])$, then the Kummer map will not be surjective [10]. It is not yet known if the necessary condition $F(\beta_1) \not\subset F(A[4])$ is also sufficient. For reducible elliptic curves, the first necessary step is to analyze the $\ell = 2$ and $\ell = 3$ cases separately and for each, explicitly compute $H^1(G_{T_n/F}, A[\ell])$. This will dictate the possible images of the arboreal representation. Once these possible images are known, $\mathcal{F}(G)$ can then be computed using the methods developed for $\ell > 3$.

6.1.2 Classes of elliptic curves with nontrivial Ш

For Type I reducible elliptic curves, computing the cohomology groups $H^1(G_{T_n/F}, E[\ell])$ has led to a project involving the Tate-Shafarevich group Ш. In particular, I determined that $H^1(G_{T_n/F}, E[\ell]) \cong (\mathbb{Z}/\ell)^2$ and further, found two generators. For $F = \mathbb{Q}$, one generator is defined by the map $M \mapsto \left(\begin{smallmatrix} a_1(M) \\ c_1(M) \end{smallmatrix}\right)$ and comes from $E(\mathbb{Q})/\ell E(\mathbb{Q})$. The other generator, ξ, is defined by $M \mapsto \left(\begin{smallmatrix} \log(\det(M)) \\ 0 \end{smallmatrix}\right)$, where log is the discrete logarithm. For rank zero elliptic curves, ξ is (by inflation) a nontrivial element of $H^1(G_{\bar{\mathbb{Q}}/\mathbb{Q}}, E[\ell])$ that does not come from $E(\mathbb{Q})/\ell E(\mathbb{Q})$. Thus, if it can be shown that this generator is in the Selmer group, a nontrivial element of Ш will be produced. By imposing the condition that the bad primes, $p \neq \ell$ of the rank zero elliptic curve E satisfy $p \equiv 1 \pmod{\ell}$, determining whether or not this element is in the Selmer group is equivalent to determining whether or not a homogeneous space has a $\mathbb{Q}_\ell$ solution. Determining necessary and sufficient conditions for when a solution exists would produce an entire class of rank zero elliptic curves with nontrivial Ш.

I have collected data for the $\ell = 3, 5$ cases and found that there are a substantial number of curves that meet the imposed conditions and have nontrivial Ш$[\ell]$ (see Appendix B). Furthermore, I have begun investigating the $\ell = 3$ case. Specifically, the elliptic curve $E(m, n)$: $y^2 + mxy + ny = x^3$ has the three-torsion point $(0, 0)$. Determining the associated homogeneous space hinges on computing the subfield of $\bar{\mathbb{Q}}(x, y)$ invariant under the map given by $x \mapsto -ny/x^2$, $y \mapsto -n^2y/x^3$, $\zeta_9 \mapsto \zeta_9^2$. I plan to continue work on determining this fixed field, thereby providing a class (depending on m and n) of rank zero elliptic curves with nontrivial Ш[3]. I will then examine the $\ell = 5$ and $\ell = 7$ cases over $\mathbb{Q}$.

6.1.3 Images of the torsion representation

A well-known theorem of Serre's states that for an elliptic curve without complex multiplication, the torsion representation is surjective for almost all ℓ [20]. The result relies on the observation that if the image of $G_{T_1/F}$ contains $\mathrm{SL}_2(\mathbb{Z}/\ell)$, then the image of $G_{T_\infty/F}$ must contain all of $\mathrm{SL}_2(\mathbb{Z}_\ell)$. If F is linearly disjoint with $\mathbb{Q}(\zeta_{\ell^n})$ for all n, this implies the torsion representation surjects onto all of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.

I would like to employ a Serre-type argument to determine when a given elliptic curve E/F with an ℓ-torsion point defined over F (resp. an $G_{\bar{\mathbb{Q}}/\mathbb{Q}}$-invariant subgroup of $E[\ell]$ of size ℓ) will

be of Type I (resp. Type II). In particular, if E is of Type I, then it is certainly necessary that $\mathrm{im}\rho_{\ell^n} = \{M \in \mathrm{GL}_2(\mathbb{Z}/\ell^n) : M \equiv \left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right) \pmod{\ell}\}$ for all n, but is this condition always sufficient for a particular (small) value of n? A related question that may be asked is how "likely" is it that E/F is a reducible elliptic curve of Type I, given that it has an ℓ torsion point defined over F? Similar questions can be asked for Type II reducible elliptic curves.

6.2 Product of Elliptic Curves

Other short-term goals include studying the arboreal representation of some other special classes of higher dimensional abelian varieties. For example, a natural follow-up to the study of products of elliptic curves with complex multiplication is to consider products of non-CM elliptic curves. The possible images of the torsion representation for two such curves was considered by Serre in [18], but controlling the amount of intersection of the torsion fields for more than two curves could be very difficult.

For A the product of m elliptic curves with complex multiplication, I would also like to investigate further when these curves have appropriately intersecting torsion fields, beginning with the $m = 2$ case. Since there are very few non-isomorphic elliptic curves over $\mathbb{Q}$ with complex multiplication, we can ask if the prescribed intersection conditions are satisfied for any two such elliptic curves for almost all ℓ. Once that is determined, we may then try to determine the largest m for which the intersection conditions are satisfied for almost all ℓ.

6.3 Abelian Surfaces with Real Multiplication

6.3.1 Higher dimensional abelian varieties

There are a number of ways to expand upon the methods developed in my thesis for abelian varieties of higher dimension. For example, Ribet's theorem can be applied to other higher dimensional abelian varieties with real multiplication, allowing the torsion representation to similarly be injected into a subgroup of two by two matrices. Though the density computation becomes exceptionally more difficult as the entries of the matrices come from larger rings, like in the case of abelian surfaces with real multiplication, the tools developed by Jones and Rouse in [10] can be modified and employed. My work with abelian surfaces with real multiplication may also extend

to abelian surfaces with complex multiplication.

Still, the methods of [10] will not work for a general abelian variety. As a long-term objective, I would therefore like to develop new techniques for studying the possible images of the arboreal representation and the density $\mathcal{F}(G)$. To begin, I would like to analyze the abelian surface case in which the image of the torsion representation is all of $\mathrm{GSp}_4(\mathbb{Z}_\ell)$. Since the main difficulty is working with four by four matrices, I would like to use the block matrix description of $\mathrm{Sp}_4(\mathbb{Z}_\ell)$ to translate the problem back to over two by two matrices. Specifically, for $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right)$, where A, B, C, D are two by two matrices, we have M is in $\mathrm{Sp}_4(\mathbb{Z}_\ell)$ if and only if $A^T D - C^T B = I$, $A^T C = C^T A$, and $D^T B = B^T D$. Since we are interested in the index of the image of $M - I$, which is given by the order ℓ valuation of $\det(M - I)$, the goal is to study this determinant in terms of the matrices A, B, C, D.

In addition, there are a number of computational techniques that can be employed to obtain bounds for $\mathcal{F}(G)$. For example, for (small) choices of ℓ and n, a Monte Carlo approach can used to give an upper bound by iteratively choosing a random pair $(v, M) \in (\mathbb{Z}/\ell^n)^{2d} \times \mathrm{GSp}_{2d}(\mathbb{Z}/\ell^n)$ and recording the portion of which satisfy $v \in \mathrm{im}(M - I)$.

A P P E N D I X

SAGE COMPUTATIONS

Cusp Forms of Level 23

input: dimension_cusp_forms(Gamma0(23),2)

output: 2

input: M = CuspForms(Gamma0(23),2,prec=100)

M.basis()

output: $[q - q^3 - q^4 - 2q^6 + 2q^7 - q^8 + 2q^9 + 2q^{10} - 4q^{11} + 3q^{12} + 3q^{13} + 2q^{14} - 4q^{15} +$
$2q^{17} - 2q^{19} - 2q^{20} - 6q^{21} - 2q^{22} + q^{23} + 5q^{24} - q^{25} + q^{27} - 4q^{28} - 3q^{29} + 2q^{30} +$
$3q^{31} + 5q^{32} + 8q^{33} - 2q^{34} + 4q^{35} - 2q^{36} - 3q^{39} - 4q^{40} - q^{41} - 2q^{42} + 6q^{44} - q^{47} -$
$6q^{48} + q^{49} - 4q^{50} + 2q^{51} - 3q^{52} - 2q^{53} + 2q^{54} - 4q^{55} - 6q^{56} + 2q^{57} + 4q^{59} + 2q^{60} -$
$2q^{61} + 6q^{62} + 4q^{63} + q^{64} + 6q^{66} - 4q^{67} - q^{69} + 11q^{71} - 2q^{72} + 9q^{73} - 2q^{74} + 9q^{75} +$
$2q^{76} - 12q^{77} - 6q^{78} - 6q^{79} + 6q^{80} - 11q^{81} - 4q^{82} - 10q^{83} + 8q^{84} - 4q^{85} + 3q^{87} +$
$8q^{88} - 8q^{89} + 4q^{90} + 6q^{91} - q^{92} - 15q^{93} - 2q^{94} - 7q^{96} + 14q^{97} + 4q^{98} - 8q^{99} +$
$O(q^{100}),$
$q^2 - 2q^3 - q^4 + 2q^5 + q^6 + 2q^7 - 2q^8 - 2q^{10} - 2q^{11} + q^{12} + 2q^{15} + 3q^{16} - 2q^{17} +$
$2q^{18} - 2q^{21} - 2q^{22} - 4q^{25} + 3q^{26} + 2q^{27} - 2q^{28} - 6q^{30} + 6q^{31} + q^{32} + 6q^{33} + 4q^{34} -$
$2q^{36} - 2q^{37} - 2q^{38} - 6q^{39} + 2q^{40} - 4q^{41} - 4q^{42} + 4q^{44} + 4q^{45} + q^{46} - 2q^{47} + 3q^{48} +$
$4q^{49} + 3q^{50} - 6q^{51} - 3q^{52} + 4q^{53} - q^{54} - 4q^{55} - 2q^{56} + 4q^{57} - 3q^{58} + 4q^{59} + 4q^{60} -$
$8q^{61} - 3q^{62} + 4q^{63} - 2q^{64} + 6q^{65} + 2q^{66} + 2q^{67} - 2q^{68} - 2q^{69} + 4q^{70} + 2q^{71} - 4q^{72} -$
$4q^{73} + 2q^{74} - 2q^{75} + 2q^{76} - 8q^{77} + 3q^{78} - 8q^{79} - 6q^{80} + 3q^{82} + 2q^{83} + 6q^{84} + 8q^{85} +$
$6q^{87} + 6q^{88} - 4q^{89} - 4q^{90} + 6q^{91} - q^{92} + q^{94} - 4q^{95} - 9q^{96} + 6q^{97} - 3q^{98} - 4q^{99} +$
$O(q^{100})]$

Nontrivial Tate-Shafarevich Groups for Elliptic Curves with ℓ Torsion

For a rank zero elliptic curve with an ℓ-torsion over $\mathbb{Q}$, if the bad primes (excluding ℓ) are congruent to 1 (mod ℓ), then the Tate-Shafarevich group being nontrivial is equivalent to there being a $\mathbb{Q}_\ell$ point on a particular homogeneous space (see Section 6.1). In this section, we compile data to support this claim for the cases $\ell = 3$ and $\ell = 5$.

By [9], the elliptic curve $E(m, n) : y^2 + mxy + ny = x^3$ has 3-torsion point $(0, 0)$. The code below for $\ell = 3$ and various choices of $mMin$, $mMax$, $nMin$, $nMax$ were used to construct Tables 1-7 that follow.

```
input:      ell = 3;
            mMin = ;
            mMax = ;
            nMin = ;
            nMax = ;
            for m in range(mMin, mMax):
              for n in range(nMin, nMax):
                if m^3 * n^3 - 27 * n^4 != 0:
                  e = EllipticCurve([m,0,n,0,0]);
                  d = e.discriminant();
                  test = 1;
                  for i in range(len(prime_divisors(d))):
                    if prime_divisors(d)[i]%ell not in[0, 1] :
                      test = 0;
                      break;
                  if test == 1:
                    if e.analytic_rank() < 1:
                      print(e.ainvs(), factor(d), e.sha().an(descent_second_limit = 16))
```

By [9], the elliptic curve $E(b) : y^2 + (1-b)xy - by = x^3 - bx^2$, $b \neq 0$, has 5-torsion point $(0, 0)$. The code below for $\ell = 5$ and various choices of $bMin$, $bMax$ were used to construct Tables 8-9 that follow.

```
input:      ell = 5;
            bMin =  ;
            bMax =  ;
            for b in range(bMin, bMax):
              e = EllipticCurve([m,0,n,0,0]);
              d = e.discriminant();
              test = 1;
              for i in range(len(prime_divisors(d))):
                if prime_divisors(d)[i]%ell not in [0, 1]
                  test = 0;
                  break;
              if test == 1:
                if e.analytic_rank() < 1:
                  print(e.ainvs(), factor(d), e.sha().an(descent_second_limit = 16))
```

Table 1. Nontrivial Ш, $\ell = 3$, $-100 \leq m \leq -50$, $1 \leq n \leq 100$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial Ш[3]?**
(-100, 0, 19, 0, 0)	$19^3 * 307 * 3259$	9	Yes
(-100, 0, 27, 0, 0)	$3^9 * 109 * 9181$	1	No
(-100, 0, 91, 0, 0)	$7^3 * 13^3 * 1002457$	1	No
(-100, 0, 93, 0, 0)	$3^3 * 31^3 * 1002511$	1	No
(-96, 0, 13, 0, 0)	$3^4 * 7^2 * 13^3 * 223$	9	Yes
(-94, 0, 39, 0, 0)	$3^3 * 13^3 * 31 * 139 * 193$	9	Yes
(-94, 0, 57, 0, 0)	$3^3 * 19^3 * 832123$	9	Yes
(-90, 0, 9, 0, 0)	$3^{11} * 3001$	9	Yes
(-90, 0, 21, 0, 0)	$3^7 * 7^3 * 9007$	4	No
(-90, 0, 39, 0, 0)	$3^7 * 13^3 * 9013$	1	No
(-90, 0, 73, 0, 0)	$3^3 * 73^3 * 27073$	9	Yes
(-88, 0, 3, 0, 0)	$3^3 * 61 * 11173$	9	Yes
(-88, 0, 31, 0, 0)	$19 * 31^3 * 35911$	9	Yes
(-88, 0, 93, 0, 0)	$3^3 * 31^3 * 683983$	4	No
(-84, 0, 57, 0, 0)	$3^6 * 13 * 19^3 * 1693$	9	Yes
(-82, 0, 9, 0, 0)	$3^6 * 67 * 8233$	9	Yes
(-78, 0, 1, 0, 0)	$3^7 * 7 * 31$	9	Yes
(-76, 0, 13, 0, 0)	$7 * 13^3 * 62761$	9	Yes
(-76, 0, 63, 0, 0)	$3^6 * 7^3 * 440677$	1	No
(-72, 0, 39, 0, 0)	$3^7 * 13^3 * 4621$	1	No
(-72, 0, 93, 0, 0)	$3^7 * 31^3 * 4639$	1	No
(-70, 0, 1, 0, 0)	$37 * 73 * 127$	9	Yes
(-70, 0, 31, 0, 0)	$13 * 31^3 * 26449$	9	Yes
(-70, 0, 39, 0, 0)	$3^3 * 13^3 * 344053$	4	No
(-70, 0, 67, 0, 0)	$67^3 * 499 * 691$	9	Yes
(-70, 0, 93, 0, 0)	$3^3 * 31^3 * 345511$	4	No
(-66, 0, 3, 0, 0)	$3^6 * 10651$	9	Yes
(-66, 0, 63, 0, 0)	$3^9 * 7^3 * 10711$	1	No
(-64, 0, 7, 0, 0)	$7^3 * 19 * 13807$	9	Yes
(-64, 0, 57, 0, 0)	$3^3 * 7 * 19^3 * 139 * 271$	9	Yes
(-64, 0, 91, 0, 0)	$7^3 * 13^3 * 264601$	1	No
(-58, 0, 1, 0, 0)	$7 * 61 * 457$	9	Yes
(-58, 0, 31, 0, 0)	$13 * 31^3 * 15073$	9	Yes
(-58, 0, 91, 0, 0)	$7^3 * 13^3 * 197569$	1	No
(-54, 0, 1, 0, 0)	$3^3 * 19 * 307$	9	Yes
(-54, 0, 21, 0, 0)	$3^7 * 7^3 * 1951$	1	No
(-54, 0, 27, 0, 0)	$3^{15} * 7 * 31$	9	Yes
(-52, 0, 79, 0, 0)	$79^3 * 349 * 409$	9	Yes

Table 2. Nontrivial Ш, $\ell = 3$, $-50 < m < 0$, $1 \leq n \leq 100$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial** $Ш[3]$**?**
(-48, 0, 63, 0, 0)	$3^9 * 7^3 * 4159$	1	No
(-46, 0, 3, 0, 0)	$3^3 * 61 * 1597$	9	Yes
(-46, 0, 39, 0, 0)	$3^3 * 13^3 * 98389$	1	No
(-46, 0, 43, 0, 0)	$7 * 43^3 * 14071$	9	Yes
(-46, 0, 91, 0, 0)	$7^3 * 13^3 * 99793$	1	No
(-42, 0, 19, 0, 0)	$3^5 * 19^3 * 307$	9	Yes
(-42, 0, 49, 0, 0)	$3^4 * 7^8 * 19$	9	Yes
(-42, 0, 73, 0, 0)	$3^5 * 73^3 * 313$	9	Yes
(-40, 0, 21, 0, 0)	$3^3 * 7^3 * 64567$	1	No
(-40, 0, 27, 0, 0)	$3^9 * 7^2 * 1321$	1	No
(-40, 0, 39, 0, 0)	$3^3 * 13^3 * 65053$	1	No
(-40, 0, 57, 0, 0)	$3^3 * 19^3 * 65539$	1	No
(-40, 0, 63, 0, 0)	$3^6 * 7^3 * 65701$	1	No
(-40, 0, 91, 0, 0)	$7^3 * 13^3 * 66457$	1	No
(-36, 0, 73, 0, 0)	$3^3 * 73^3 * 1801$	9	Yes
(-36, 0, 93, 0, 0)	$3^7 * 31^3 * 607$	1	No
(-34, 0, 39, 0, 0)	$3^3 * 13^3 * 40357$	4	No
(-30, 0, 63, 0, 0)	$3^9 * 7^3 * 1063$	1	No
(-28, 0, 27, 0, 0)	$3^9 * 37 * 613$	1	No
(-28, 0, 31, 0, 0)	$13 * 31^3 * 1753$	9	Yes
(-24, 0, 37, 0, 0)	$3^5 * 37^3 * 61$	9	Yes
(-22, 0, 27, 0, 0)	$3^9 * 31 * 367$	1	No
(-22, 0, 39, 0, 0)	$3^3 * 13^3 * 11701$	1	No
(-22, 0, 93, 0, 0)	$3^3 * 31^3 * 13159$	1	No
(-18, 0, 1, 0, 0)	$3^3 * 7 * 31$	9	Yes
(-18, 0, 21, 0, 0)	$3^7 * 7^3 * 79$	1	No
(-18, 0, 27, 0, 0)	3^{17}	1	No
(-18, 0, 31, 0, 0)	$3^3 * 13 * 19 * 31^3$	9	Yes
(-16, 0, 21, 0, 0)	$3^3 * 7^3 * 4663$	1	No
(-16, 0, 91, 0, 0)	$7^3 * 13^3 * 6553$	1	No
(-16, 0, 93, 0, 0)	$3^3 * 31^3 * 6607$	1	No
(-12, 0, 63, 0, 0)	$3^9 * 7^3 * 127$	1	No
(-10, 0, 21, 0, 0)	$3^3 * 7^3 * 1567$	1	No
(-10, 0, 39, 0, 0)	$3^3 * 13^3 * 2053$	1	No
(-10, 0, 57, 0, 0)	$3^3 * 19^3 * 2539$	1	No
(-10, 0, 91, 0, 0)	$7^3 * 13^3 * 3457$	1	No
(-10, 0, 93, 0, 0)	$3^3 * 31^3 * 3511$	1	No
(-6, 0, 1, 0, 0)	3^5	1	No
(-4, 0, 21, 0, 0)	$3^3 * 7^3 * 631$	1	No
(-4, 0, 27, 0, 0)	$3^9 * 13 * 61$	1	No
(-4, 0, 91, 0, 0)	$7^3 * 13^3 * 2521$	1	No

Table 3. Nontrivial Ш, $\ell = 3$, $10 \leq m \leq 50$, $1 \leq n \leq 100$

Elliptic Curve	Discriminant	$\lvert Ш \rvert$	Nontrivial Ш[3]?
(10, 0, 21, 0, 0)	$3^3 * 7^3 * 433$	1	No
(10, 0, 37, 0, 0)	37^3	1	No
(12, 0, 1, 0, 0)	$3^5 * 7$	1	No
(12, 0, 21, 0, 0)	$3^6 * 7^3 * 43$	1	No
(12, 0, 27, 0, 0)	$3^{12} * 37$	1	No
(12, 0, 57, 0, 0)	$3^6 * 7 * 19^3$	1	No
(12, 0, 61, 0, 0)	$3^4 * 61^3$	4	No
(12, 0, 67, 0, 0)	$3^4 * 67^3$	4	No
(12, 0, 91, 0, 0)	$3^6 * 7^3 * 13^3$	1	No
(16, 0, 37, 0, 0)	$19 * 37^3 * 163$	9	Yes
(16, 0, 57, 0, 0)	$3^3 * 19^3 * 2557$	1	No
(16, 0, 97, 0, 0)	$7 * 97^3 * 211$	9	Yes
(22, 0, 1, 0, 0)	$13 * 19 * 43$	9	Yes
(22, 0, 91, 0, 0)	$7^3 * 13^3 * 8191$	1	No
(24, 0, 1, 0, 0)	$3^3 * 7 * 73$	9	Yes
(24, 0, 43, 0, 0)	$3^3 * 7 * 43^3 * 67$	9	Yes
(24, 0, 73, 0, 0)	$3^3 * 73^3 * 439$	9	Yes
(28, 0, 27, 0, 0)	$3^9 * 19 * 1117$	1	No
(28, 0, 39, 0, 0)	$3^3 * 13^3 * 20899$	4	No
(28, 0, 49, 0, 0)	$7^8 * 421$	9	Yes
(30, 0, 39, 0, 0)	$3^6 * 13^3 * 31^2$	1	No
(30, 0, 63, 0, 0)	$3^9 * 7^3 * 937$	1	No
(30, 0, 93, 0, 0)	$3^6 * 31^3 * 907$	1	No
(30, 0, 97, 0, 0)	$3^4 * 7 * 43 * 97^3$	9	Yes
(34, 0, 1, 0, 0)	$7 * 31 * 181$	9	Yes
(34, 0, 3, 0, 0)	$3^3 * 61 * 643$	9	Yes
(34, 0, 21, 0, 0)	$3^3 * 7^3 * 38737$	1	No
(34, 0, 43, 0, 0)	$7 * 43^3 * 5449$	9	Yes
(34, 0, 73, 0, 0)	$37 * 73^3 * 1009$	9	Yes
(34, 0, 93, 0, 0)	$3^3 * 31^3 * 36793$	4	No
(36, 0, 27, 0, 0)	$3^{17} * 7$	1	No
(40, 0, 79, 0, 0)	$13 * 79^3 * 4759$	9	Yes
(40, 0, 91, 0, 0)	$7^3 * 13^3 * 61543$	1	No
(42, 0, 1, 0, 0)	$3^3 * 13 * 211$	9	Yes
(42, 0, 73, 0, 0)	$3^3 * 73^3 * 2671$	9	Yes
(42, 0, 91, 0, 0)	$3^3 * 7^4 * 13^3 * 379$	9	Yes
(46, 0, 1, 0, 0)	$31 * 43 * 73$	9	Yes
(46, 0, 7, 0, 0)	$7^3 * 19 * 5113$	9	Yes
(48, 0, 9, 0, 0)	$3^9 * 61 * 67$	9	Yes
(48, 0, 19, 0, 0)	$3^6 * 19^3 * 151$	9	Yes
(48, 0, 79, 0, 0)	$3^4 * 13 * 79^3 * 103$	9	Yes
(48, 0, 93, 0, 0)	$3^6 * 31^3 * 4003$	1	No
(48, 0, 97, 0, 0)	$3^4 * 31 * 43 * 97^3$	9	Yes

Table 4. Nontrivial Ш, $\ell = 3$, $50 < m \leq 100$, $1 \leq n \leq 100$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial** $Ш[3]$**?**
(52, 0, 1, 0, 0)	$7^2 * 19 * 151$	9	Yes
(52, 0, 27, 0, 0)	$3^9 * 43 * 3253$	1	No
(52, 0, 61, 0, 0)	$61^3 * 79 * 1759$	9	Yes
(58, 0, 13, 0, 0)	$7 * 13^3 * 27823$	9	Yes
(58, 0, 27, 0, 0)	$3^9 * 7^2 * 3967$	1	No
(58, 0, 57, 0, 0)	$3^3 * 19^3 * 193573$	4	No
(60, 0, 1, 0, 0)	$3^3 * 19 * 421$	9	Yes
(60, 0, 37, 0, 0)	$3^3 * 37^3 * 7963$	9	Yes
(60, 0, 43, 0, 0)	$3^3 * 43^3 * 73 * 109$	9	Yes
(64, 0, 21, 0, 0)	$3^3 * 7^3 * 261577$	1	No
(64, 0, 73, 0, 0)	$73^3 * 151 * 1723$	9	Yes
(66, 0, 21, 0, 0)	$3^6 * 7^3 * 10627$	1	No
(66, 0, 27, 0, 0)	$3^{12} * 13 * 19 * 43$	9	Yes
(66, 0, 79, 0, 0)	$3^4 * 13 * 79^3 * 271$	9	Yes
(70, 0, 3, 0, 0)	$3^3 * 307 * 1117$	9	Yes
(70, 0, 7, 0, 0)	$7^4 * 48973$	9	Yes
(70, 0, 39, 0, 0)	$3^3 * 13^3 * 341947$	1	No
(70, 0, 57, 0, 0)	$3^3 * 19^3 * 341461$	1	No
(72, 0, 27, 0, 0)	$3^{15} * 7 * 73$	9	Yes
(76, 0, 21, 0, 0)	$3^3 * 7^3 * 438409$	4	No
(76, 0, 39, 0, 0)	$3^3 * 13^3 * 437923$	1	No
(76, 0, 61, 0, 0)	$61^3 * 163 * 2683$	9	Yes
(78, 0, 37, 0, 0)	$3^3 * 37^3 * 17539$	9	Yes
(82, 0, 1, 0, 0)	$7 * 79 * 997$	9	Yes
(82, 0, 21, 0, 0)	$3^3 * 7^3 * 550801$	4	No
(82, 0, 61, 0, 0)	$61^3 * 241 * 2281$	36	Yes
(84, 0, 43, 0, 0)	$3^4 * 43^3 * 67 * 109$	9	Yes
(88, 0, 13, 0, 0)	$7 * 13^3 * 97303$	9	Yes
(88, 0, 37, 0, 0)	$37^3 * 457 * 1489$	9	Yes
(88, 0, 57, 0, 0)	$3^3 * 19^3 * 679933$	4	No
(94, 0, 21, 0, 0)	$3^3 * 7^3 * 830017$	4	No
(94, 0, 79, 0, 0)	$13 * 79^3 * 63727$	9	Yes
(96, 0, 97, 0, 0)	$3^3 * 37 * 97^3 * 883$	9	Yes

Table 5. Nontrivial Ш, $\ell = 3$, $400 \leq m \leq 406$, $1 \leq n \leq 500$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial Ш[3]?**
(400, 0, 1, 0, 0)	$37 * 397 * 4357$	36	Yes
(400, 0, 49, 0, 0)	$7^6 * 541 * 118297$	9	Yes
(400, 0, 63, 0, 0)	$3^6 * 7^3 * 63998299$	4	No
(400, 0, 97, 0, 0)	$7^2 * 97^3 * 1306069$	9	Yes
(400, 0, 199, 0, 0)	$139 * 199^3 * 460393$	9	Yes
(400, 0, 201, 0, 0)	$3^3 * 67^3 * 63994573$	9	Yes
(400, 0, 217, 0, 0)	$7^3 * 31^3 * 63994141$	9	Yes
(400, 0, 223, 0, 0)	$7 * 37 * 211 * 223^3 * 1171$	81	Yes
(400, 0, 271, 0, 0)	$271^3 * 1297 * 49339$	9	Yes
(400, 0, 273, 0, 0)	$3^3 * 7^3 * 13^3 * 199 * 321571$	1	No
(400, 0, 291, 0, 0)	$3^3 * 97^3 * 63992143$	36	Yes
(400, 0, 307, 0, 0)	$7 * 307^3 * 9141673$	9	Yes
(400, 0, 313, 0, 0)	$313^3 * 7039 * 9091$	9	Yes
(400, 0, 327, 0, 0)	$3^3 * 109^3 * 63991171$	9	Yes
(400, 0, 351, 0, 0)	$3^9 * 13^3 * 63990523$	1	No
(400, 0, 361, 0, 0)	$19^6 * 5821 * 10993$	36	Yes
(400, 0, 421, 0, 0)	$241 * 421^3 * 265513$	9	Yes
(400, 0, 463, 0, 0)	$463^3 * 1093 * 58543$	9	Yes
(400, 0, 471, 0, 0)	$3^3 * 157^3 * 63987283$	64	No
(400, 0, 489, 0, 0)	$3^3 * 7^2 * 163^3 * 877 * 1489$	9	Yes
(402, 0, 1, 0, 0)	$3^3 * 7 * 19 * 79 * 229$	81	Yes
(402, 0, 31, 0, 0)	$3^3 * 31^3 * 37 * 65029$	36	Yes
(402, 0, 133, 0, 0)	$3^3 * 7^3 * 19^3 * 2405971$	1	No
(402, 0, 271, 0, 0)	$3^3 * 271^3 * 2405833$	9	Yes
(402, 0, 307, 0, 0)	$3^3 * 307^3 * 2405797$	36	Yes
(402, 0, 343, 0, 0)	$3^3 * 7^9 * 19 * 127 * 997$	36	Yes
(402, 0, 397, 0, 0)	$3^3 * 397^3 * 2405707$	36	Yes
(402, 0, 403, 0, 0)	$3^3 * 13^3 * 31^3 * 2405701$	16	No
(402, 0, 427, 0, 0)	$3^3 * 7^3 * 61^3 * 2405677$	1	No
(402, 0, 457, 0, 0)	$3^3 * 19 * 457^3 * 126613$	9	Yes
(406, 0, 7, 0, 0)	$7^4 * 9560461$	9	Yes
(406, 0, 111, 0, 0)	$3^3 * 37^3 * 66920419$	1	No
(406, 0, 129, 0, 0)	$3^3 * 43^3 * 66919933$	9	Yes
(406, 0, 157, 0, 0)	$13 * 157^3 * 5147629$	36	Yes
(406, 0, 181, 0, 0)	$181^3 * 4597 * 14557$	9	Yes
(406, 0, 247, 0, 0)	$13^3 * 19^3 * 66916747$	9	Yes
(406, 0, 307, 0, 0)	$157 * 307^3 * 426211$	144	Yes
(406, 0, 417, 0, 0)	$3^3 * 13 * 109 * 139^3 * 47221$	81	Yes
(406, 0, 457, 0, 0)	$457^3 * 829 * 80713$	9	Yes
(406, 0, 469, 0, 0)	$7^4 * 13 * 67^3 * 735283$	9	Yes
(406, 0, 489, 0, 0)	$3^3 * 163^3 * 66910213$	1	No

Table 6. Nontrivial Ш, $\ell = 3$, $406 < m \leq 415$, $1 \leq n \leq 500$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial Ш[3]?**
(408, 0, 39, 0, 0)	$3^6 * 13^3 * 2515417$	25	No
(408, 0, 73, 0, 0)	$3^5 * 13 * 73^3 * 21499$	9	Yes
(408, 0, 117, 0, 0)	$3^9 * 13^3 * 2515339$	1	No
(408, 0, 133, 0, 0)	$3^4 * 7^3 * 19^3 * 838441$	36	Yes
(408, 0, 183, 0, 0)	$3^6 * 61^3 * 2515273$	4	No
(408, 0, 217, 0, 0)	$3^6 * 7^3 * 19 * 31^3 * 4903$	9	Yes
(408, 0, 219, 0, 0)	$3^6 * 73^3 * 2515237$	64	No
(408, 0, 223, 0, 0)	$3^4 * 7 * 223^3 * 119773$	9	Yes
(408, 0, 243, 0, 0)	$3^{18} * 61 * 41233$	9	Yes
(408, 0, 259, 0, 0)	$3^4 * 7^3 * 37^3 * 838399$	25	No
(408, 0, 309, 0, 0)	$3^6 * 103^3 * 2515147$	36	Yes
(408, 0, 313, 0, 0)	$3^4 * 313^3 * 577 * 1453$	36	Yes
(408, 0, 333, 0, 0)	$3^9 * 13 * 31 * 37^3 * 79^2$	9	Yes
(408, 0, 379, 0, 0)	$3^6 * 379^3 * 93151$	9	Yes
(408, 0, 403, 0, 0)	$3^4 * 13^3 * 31^3 * 838351$	36	Yes
(408, 0, 417, 0, 0)	$3^6 * 139^3 * 2515039$	1	No
(408, 0, 457, 0, 0)	$3^4 * 31 * 457^3 * 27043$	36	Yes
(412, 0, 27, 0, 0)	$3^9 * 13 * 31 * 97 * 1789$	9	Yes
(412, 0, 63, 0, 0)	$3^6 * 7^3 * 69932827$	4	No
(412, 0, 103, 0, 0)	$103^4 * 678949$	36	Yes
(412, 0, 111, 0, 0)	$3^3 * 37^3 * 69931531$	36	Yes
(412, 0, 133, 0, 0)	$7^3 * 19^3 * 69930937$	4	No
(412, 0, 151, 0, 0)	$31 * 151^3 * 2255821$	9	Yes
(412, 0, 163, 0, 0)	$19 * 163^3 * 3680533$	9	Yes
(412, 0, 183, 0, 0)	$3^3 * 7 * 13 * 61^3 * 768457$	9	Yes
(412, 0, 243, 0, 0)	$3^{15} * 67 * 1043701$	9	Yes
(412, 0, 273, 0, 0)	$3^3 * 7^3 * 13^3 * 4177 * 16741$	4	No
(412, 0, 277, 0, 0)	$19 * 277^3 * 3680371$	9	Yes
(412, 0, 313, 0, 0)	$13 * 313^3 * 5378929$	9	Yes
(412, 0, 387, 0, 0)	$3^6 * 43^3 * 69924079$	4	No
(412, 0, 453, 0, 0)	$3^3 * 151^3 * 69922297$	4	No
(412, 0, 471, 0, 0)	$3^3 * 157^3 * 69921811$	16	No

Table 7. Nontrivial Ш, $\ell = 3$, $415 < m \leq 425$, $1 \leq n \leq 500$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial Ш[3]?**
(418, 0, 3, 0, 0)	$3^3 * 661 * 110491$	81	Yes
(418, 0, 7, 0, 0)	$7^3 * 1087 * 67189$	9	Yes
(418, 0, 27, 0, 0)	$3^9 * 409 * 178567$	1	No
(418, 0, 43, 0, 0)	$7^2 * 43^3 * 1490479$	9	Yes
(418, 0, 73, 0, 0)	$13 * 73^3 * 5617897$	9	Yes
(418, 0, 139, 0, 0)	$73 * 139^3 * 1000423$	81	Yes
(418, 0, 147, 0, 0)	$3^3 * 7^6 * 73030663$	1	No
(418, 0, 189, 0, 0)	$3^9 * 7^3 * 73029529$	1	No
(418, 0, 193, 0, 0)	$193^3 * 211 * 346111$	9	Yes
(418, 0, 199, 0, 0)	$79 * 199^3 * 924421$	36	Yes
(418, 0, 229, 0, 0)	$13^2 * 229^3 * 432121$	36	Yes
(418, 0, 277, 0, 0)	$277^3 * 499 * 146347$	36	Yes
(418, 0, 313, 0, 0)	$67 * 313^3 * 1089943$	9	Yes
(418, 0, 337, 0, 0)	$7^2 * 337^3 * 1490317$	9	Yes
(418, 0, 343, 0, 0)	$7^9 * 397 * 183943$	1	No
(418, 0, 379, 0, 0)	$7 * 379^3 * 10432057$	9	Yes
(418, 0, 399, 0, 0)	$3^3 * 7^3 * 19^4 * 3843361$	4	No
(418, 0, 417, 0, 0)	$3^3 * 139^3 * 73023373$	4	No
(418, 0, 427, 0, 0)	$7^3 * 61^3 * 73023103$	4	No
(420, 0, 7, 0, 0)	$3^3 * 7^4 * 391999$	9	Yes
(420, 0, 79, 0, 0)	$3^3 * 79^3 * 433 * 6337$	9	Yes
(420, 0, 97, 0, 0)	$3^3 * 31 * 97^3 * 88513$	9	Yes
(420, 0, 343, 0, 0)	$3^3 * 7^{12} * 19 * 421$	9	Yes
(420, 0, 379, 0, 0)	$3^3 * 379^3 * 2743621$	9	Yes
(420, 0, 409, 0, 0)	$3^3 * 79 * 409^3 * 34729$	9	Yes
(424, 0, 1, 0, 0)	$331 * 421 * 547$	144	Yes
(424, 0, 49, 0, 0)	$7^6 * 1087 * 70123$	9	Yes
(424, 0, 79, 0, 0)	$79^3 * 97 * 785803$	81	Yes
(424, 0, 163, 0, 0)	$163^3 * 601 * 126823$	36	Yes
(424, 0, 291, 0, 0)	$3^3 * 13 * 97^3 * 1693 * 3463$	9	Yes
(424, 0, 343, 0, 0)	$7^9 * 13 * 31 * 379 * 499$	36	Yes
(424, 0, 373, 0, 0)	$103 * 373^3 * 739951$	36	Yes
(424, 0, 433, 0, 0)	$7 * 433^3 * 10887619$	9	Yes
(424, 0, 469, 0, 0)	$7^3 * 67^3 * 76212361$	25	No
(424, 0, 471, 0, 0)	$3^3 * 157^3 * 76212307$	16	No

Table 8. Nontrivial Ш, $\ell = 5$, $-10000 \leq b \leq -5000$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial** $Ш[5]$**?**
(9942, 9941, 9941, 0, 0)	$-1 * 701 * 9941^5 * 141131$	25	Yes
(9782, 9781, 9781, 0, 0)	$-1 * 61 * 9781^5 * 1570091$	25	Yes
(9522, 9521, 9521, 0, 0)	$-1 * 151 * 9521^5 * 601021$	225	Yes
(9462, 9461, 9461, 0, 0)	$-1 * 11 * 9461^5 * 8146781$	25	Yes
(9342, 9341, 9341, 0, 0)	$-1 * 4861 * 9341^5 * 17971$	225	Yes
(9242, 9241, 9241, 0, 0)	$-1 * 11 * 9241^5 * 7772521$	225	Yes
(8822, 8821, 8821, 0, 0)	$-1 * 11 * 8821^5 * 7082461$	625	Yes
(8762, 8761, 8761, 0, 0)	$-1 * 3571 * 8761^5 * 21521$	400	Yes
(8742, 8741, 8741, 0, 0)	$-1 * 1031 * 8741^5 * 74201$	1225	Yes
(8372, 8371, 8371, 0, 0)	$-1 * 11^5 * 761^5 * 70165721$	64	No
(8082, 8081, 8081, 0, 0)	$-1 * 61 * 8081^5 * 1071991$	25	Yes
(7382, 7381, 7381, 0, 0)	$-1 * 11^{10} * 61^5 * 54560351$	4	No
(7322, 7321, 7321, 0, 0)	$-1 * 691 * 7321^5 * 77681$	100	Yes
(7122, 7121, 7121, 0, 0)	$-1 * 181 * 7121^5 * 280591$	225	Yes
(6842, 6841, 6841, 0, 0)	$-1 * 11 * 6841^5 * 4261321$	100	Yes
(6792, 6791, 6791, 0, 0)	$-1 * 521 * 6791^5 * 88661$	400	Yes
(6582, 6581, 6581, 0, 0)	$-1 * 271 * 6581^5 * 160081$	25	Yes
(6572, 6571, 6571, 0, 0)	$-1 * 101 * 6571^5 * 428221$	1600	Yes
(6552, 6551, 6551, 0, 0)	$-1 * 281 * 6551^5 * 152981$	100	Yes
(6492, 6491, 6491, 0, 0)	$-1 * 11 * 6491^5 * 3836771$	100	Yes
(6422, 6421, 6421, 0, 0)	$-1 * 2971 * 6421^5 * 13901$	625	Yes
(6312, 6311, 6311, 0, 0)	$-1 * 1811 * 6311^5 * 22031$	1600	Yes
(6282, 6281, 6281, 0, 0)	$-1 * 11^5 * 571^5 * 39520051$	16	No
(6192, 6191, 6191, 0, 0)	$-1 * 41^5 * 151^5 * 38396581$	16	No
(6102, 6101, 6101, 0, 0)	$-1 * 31 * 6101^5 * 1202881$	225	Yes
(5922, 5921, 5921, 0, 0)	$-1 * 31^5 * 191^5 * 35123371$	36	No
(5792, 5791, 5791, 0, 0)	$-1 * 31 * 5791^5 * 1083851$	100	Yes
(5732, 5731, 5731, 0, 0)	$-1 * 11^5 * 521^5 * 32907401$	4	No
(5522, 5521, 5521, 0, 0)	$-1 * 11 * 41 * 241 * 281 * 5521^5$	625	Yes
(5432, 5431, 5431, 0, 0)	$-1 * 251 * 5431^5 * 117751$	100	Yes
(5372, 5371, 5371, 0, 0)	$-1 * 41^5 * 131^5 * 28906721$	16	No
(5352, 5351, 5351, 0, 0)	$-1 * 251 * 5351^5 * 114311$	100	Yes
(5052, 5051, 5051, 0, 0)	$-1 * 401 * 5051^5 * 63761$	100	Yes

Table 9. Nontrivial Ш, $\ell = 5$, $-5000 \leq b \leq -1$

Elliptic Curve	**Discriminant**	$\lvert Ш \rvert$	**Nontrivial** $Ш[5]$**?**
(4722, 4721, 4721, 0, 0)	$-1 * 601 * 4721^5 * 37171$	25	Yes
(4652, 4651, 4651, 0, 0)	$-1 * 1031 * 4651^5 * 21031$	100	Yes
(4332, 4331, 4331, 0, 0)	$-1 * 61^5 * 71^5 * 18805201$	64	No
(4242, 4241, 4241, 0, 0)	$-1 * 31 * 4241^5 * 581701$	25	Yes
(4232, 4231, 4231, 0, 0)	$-1 * 2221 * 4231^5 * 8081$	100	Yes
(4212, 4211, 4211, 0, 0)	$-1 * 31 * 4211^5 * 573511$	100	Yes
(4062, 4061, 4061, 0, 0)	$-1 * 31^5 * 131^5 * 16536391$	4	No
(4022, 4021, 4021, 0, 0)	$-1 * 41 * 4021^5 * 395431$	400	Yes
(4002, 4001, 4001, 0, 0)	$-1 * 541 * 4001^5 * 29671$	225	Yes
(3882, 3881, 3881, 0, 0)	$-1 * 41 * 3881^5 * 368411$	25	Yes
(3632, 3631, 3631, 0, 0)	$-1 * 11 * 3631^5 * 1202191$	100	Yes
(3192, 3191, 3191, 0, 0)	$-1 * 11 * 3191^5 * 928871$	100	Yes
(3092, 3091, 3091, 0, 0)	$-1 * 11^5 * 281^5 * 9588281$	16	No
(3062, 3061, 3061, 0, 0)	$-1 * 41 * 3061^5 * 229351$	25	Yes
(3012, 3011, 3011, 0, 0)	$-1 * 971 * 3011^5 * 9371$	100	Yes
(2862, 2861, 2861, 0, 0)	$-1 * 11 * 2861^5 * 746981$	25	Yes
(2622, 2621, 2621, 0, 0)	$-1 * 941 * 2621^5 * 7331$	25	Yes
(2322, 2321, 2321, 0, 0)	$-1 * 11^5 * 211^5 * 5412571$	16	No
(2112, 2111, 2111, 0, 0)	$-1 * 11^2 * 2111^5 * 37021$	100	Yes
(2102, 2101, 2101, 0, 0)	$-1 * 11^5 * 191^5 * 4437311$	1	No
(1872, 1871, 1871, 0, 0)	$-1 * 11^2 * 1871^5 * 29101$	100	Yes
(1832, 1831, 1831, 0, 0)	$-1 * 41 * 1831^5 * 82261$	100	Yes
(1742, 1741, 1741, 0, 0)	$-1 * 71 * 1741^5 * 42961$	225	Yes
(1532, 1531, 1531, 0, 0)	$-1 * 311 * 1531^5 * 7591$	100	Yes
(1482, 1481, 1481, 0, 0)	$-1 * 1181 * 1481^5 * 1871$	25	Yes
(1202, 1201, 1201, 0, 0)	$-1 * 191 * 1201^5 * 7621$	25	Yes
(762, 761, 761, 0, 0)	$-1 * 61 * 761^5 * 9631$	25	Yes
(672, 671, 671, 0, 0)	$-1 * 11^5 * 61^5 * 457621$	4	No
(662, 661, 661, 0, 0)	$-1 * 11^2 * 661^5 * 3671$	25	Yes
(522, 521, 521, 0, 0)	$-1 * 31 * 521^5 * 8941$	25	Yes

BIBLIOGRAPHY

[1] Emil Artin. *The collected papers of Emil Artin*. Edited by Serge Lang and John T. Tate. Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965.

[2] Daniel Bump, Solomon Friedberg, and Jeffrey Hoffstein. Eisenstein series on the metaplectic group and nonvanishing theorems for automorphic L-functions and their derivatives. *Ann. of Math. (2)*, 131(1):53–127, 1990.

[3] John Cullinan. Personal communication, February 28, 2012.

[4] Rajiv Gupta and M. Ram Murty. A remark on Artin's conjecture. *Invent. Math.*, 78(1):127–130, 1984.

[5] Helmut Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von durch eine vorgegebene Primzahl $l \neq 2$ *teilbarer bzw. unteilbarer* Ordnung mod. p ist. *Math. Ann.*, 162:74–76, 1965/1966.

[6] Helmut Hasse. Über die Dichte der Primzahlen p, für die eine vorgegebene ganzrationale Zahl $a \neq 0$ von gerader bzw.ungerader Ordnung mod. p ist. *Math. Ann.*, 166:19–23, 1966.

[7] D. R. Heath-Brown. Artin's conjecture for primitive roots. *Quart. J. Math. Oxford Ser. (2)*, 37(145):27–38, 1986.

[8] Marc Hindry and Joseph H. Silverman. *Diophantine geometry*, volume 201 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2000. An introduction.

[9] Dale Husemöller. *Elliptic curves*, volume 111 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, second edition, 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.

[10] Rafe Jones and Jeremy Rouse. Galois theory of iterated endomorphisms. *Proc. Lond. Math. Soc. (3)*, 100(3):763–794, 2010. Appendix A by Jeffrey D. Achter.

[11] V. A. Kolyvagin and D. Yu. Logachëv. Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties. *Algebra i Analiz*, 1(5):171–196, 1989.

[12] Douglas Andrew Kuhlman. *On the orders of Jacobians of hyperelliptic curves*. ProQuest LLC, Ann Arbor, MI, 2000. Thesis (Ph.D.)–University of Illinois at Urbana-Champaign.

[13] Pieter Moree. On primes p for which d divides $\mathrm{ord}_p(g)$. *Funct. Approx. Comment. Math.*, 33:85–95, 2005.

[14] David Mumford. *Abelian varieties*. Tata Institute of Fundamental Research Studies in Mathematics, No. 5. Published for the Tata Institute of Fundamental Research, Bombay, 1970.

[15] M. Ram Murty. Artin's conjecture for primitive roots. *Math. Intelligencer*, 10(4):59–67, 1988.

[16] M. Ram Murty and V. Kumar Murty. Mean values of derivatives of modular L-series. *Ann. of Math. (2)*, 133(3):447–475, 1991.

[17] Kenneth A. Ribet. On l-adic representations attached to modular forms. *Invent. Math.*, 28:245–275, 1975.

[18] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[19] Jean-Pierre Serre. *Œuvres. Vol. III.* Springer-Verlag, Berlin, 1986. 1972–1984.

[20] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*, volume 7 of *Research Notes in Mathematics*. A K Peters Ltd., Wellesley, MA, 1998. With the collaboration of Willem Kuyk and John Labute, Revised reprint of the 1968 original.

[21] Jean-Pierre Serre. *Œuvres. Collected papers. IV*. Springer-Verlag, Berlin, 2000. 1985–1998.

[22] Jean-Pierre Serre and John Tate. Good reduction of abelian varieties. *Ann. of Math. (2)*, 88:492–517, 1968.

[23] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, Dordrecht, second edition, 2009.

[24] H. P. F. Swinnerton-Dyer. On l-adic representations and congruences for coefficients of modular forms. In *Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972)*, pages 1–55. Lecture Notes in Math., Vol. 350. Springer, Berlin, 1973.

[25] V. M. Usenko. Subgroups of semidirect products. *Ukrain. Mat. Zh.*, 43(7-8):1048–1055, 1991.

[26] Adrian Vasiu. Surjectivity criteria for p-adic representations. II. *Manuscripta Math.*, 114(4):399–422, 2004.